T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR AĞ GÜVENLİĞİ VE GÜVENLİK DUVARLARI

Hakan ÇAKAR

YÜKSEK LİSANS TEZİ
ELEKTRONİK BİLGİSAYAR EĞİTİMİ
ANA BİLİM DALI

ELAZIĞ
2005

T.C.

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR AĞ GÜVENLİĞİ VE GÜVENLİK DUVARLARI

Hakan ÇAKAR

YÜKSEK LİSANS TEZİ

ELEKTRONİK BİLGİSAYAR EĞİTİMİ

ANA BİLİM DALI

Bu tez, 28.07.05 tarihinde aşağıda belirtilen jüri tarafından oybirliği /~~oyçokluğu~~ ile başarılı / ~~başarısız~~ olarak değerlendirilmiştir.

Üye: Yrd.Doç.Dr. Ahmet GINAR

Üye: Doç.Dr.Hanifi GÜLDEMİR

Üye: Yrd. Doç. Dr. Mehmet GEDİKPINAR

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 12/08/05 tarih ve 2005-26/11 sayılı kararıyla onaylanmıştır.

TEŞEKKÜR

Bu tez çalışmam boyunca, ilgi ve yardımlarını esirgemeyen danışmanım Sayın Prof. Dr. Asaf VAROL' a, çalışmam esnasında değerli fikir ve yardımlarından yararlandığım Öğr.Gör. Fatih TALU' ya teşekkürlerimi ve şükranlarımı sunarım.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

LAN	:Local Area Network
BSD	:Berkeley Software Distribution
DMZ	:Demilitarized Zone
TCP	:Transfer Control Protokol
UDP	:User Datagram Protokol
ICMP	:Internet Control Message Protocol
FTP	:File Transfer Protocol
OSI	:Open System Interconnection
FDDI	:Fiber Distributed Data Interface
DNS	:Domain Name System
SMTP	:Simple Mail Transfer Protocol
NFS	:Network File System
DARPA	:Department of Defense Advanced Research Projects Agency
ACK	:Acknowledgement
MAC	:Media Access Control
ARP	:Adress Resulation Protocol
DES	:Data Encryption Standart
ISA	:Internet Security and Acceleration Server
VPN	:Virtual Private Network
SSL	:Secure Socket Layer
SCSI	:Small Computer System Interface
IIS	:Internet Information Server
LAT	:Local Adres Table
DHCP	:Dynamic Host Configuration Protocol
ECC	:Elliptic Curve Cryptography
RSA	:Ron Rivest, Adi Shamir, Leonard Adleman

ÖZET

BİLGİSAYAR AĞ GÜVENLİĞİ VE GÜVENLİK DUVARLARI

Hakan ÇAKAR

Fırat Üniversitesi
Fen Bilimleri Enstitüsü
Elektronik-Bilgisayar Eğitimi Anabilim Dalı

2005, Sayfa:82

Bu tez çalışmasında, bilgisayar ağlarındaki güvenlik sorunları, güvenliği sağlama yöntemleri, saldırı türleri, korunma mekanizmaları, güvenlik sınıflamaları ve güvenlik duvarı yapısı incelenmiştir. Güvenlik duvarı uygulaması olarak ISA Server sistemi gerçekleştirilmiş, kurulan küçük ölçekli bir ağ üzerinde bu sistemin etkileri ve özellikleri incelenmiştir. Bunun yanı sıra, gerek sağladıkları yüksek güvenlik, gerekse hız faktörü nedeniyle iletişim uygulamalarında kullanılması gerekli olan RSA ve Eliptik Eğri şifreleme algoritmalarıyla ilgili bir yazılım oluşturulmuş, bu algoritmaların çalışması program üzerinde gösterilmiştir.

Anahtar Kelimeler: Güvenlik Duvarı, ISA Server, RSA Algoritması, Eliptik Eğri Algoritması

ABSTRACT

COMPUTER NETWORKS SECURITY AND FIREWALLS

Hakan ÇAKAR

Firat University
Graduate School of Natural and Applied Sciences
Department of Electronic and Computer Education

2005, Page:82

In this thesis, the security problems in computer networks, security providing methods, attack types, protection mechanisms, security classifications and firewall structure were examined. ISA Server system was realized as firewall application. Effects and features of this system were investigated on an assembled little scale network. Furthermore, a software related to RSA and Elliptic Curve Encryption algorithms that provide high security and speed in communication applications has been prepared and the running of these algorithms has been demonstrated in this software.

Keywords: Firewall, ISA Server, RSA Algorithm, Elliptic Curve Algorithm

1.GİRİŞ

Bilim ve teknoloji uzun bir süre ayrı olarak yollarına devam etmişlerdir. Sanayi devrimine kadar teknoloji, mucitlerin kontrolünde daima bilimden önde gitmiştir. Ancak, sanayi devriminden sonra bilim ve teknoloji, biribirini tamamlayan kavramlar haline gelmiştir. Bu sebeple atölyelerin yerlerini, bilim adamlarının laboratuarları ve araştırma merkezleri almıştır. Bu gelişmeler, insanların sosyal hayatına ve insanların evreni algılamasında farklı bakış açılarına yönelmelerine sebep olmuştur.

MÖ. 3500 yılı civarında yazının, MÖ. 170 yılında ilk kağıt (parşömen) ve 1454 yılında da matbaanın icadı ile bilgi yeni bir boyutta gelişme gösterirken; daktilo, telgraf, telefon, sabit resimlerin elektromanyetik dalga ile dijital halde iletimi, televizyon yayını, haberleşme uydusu, denizaşırı fiber optik kablo ile yazılı metinlerin yanında ses ve hareketli görüntüyü de kapsayan Internet' in ortaya çıkması ile bilgi yeni bir boyut kazanmıştır. Haberleşme teknolojilerinin gelişmesi sayesinde bilginin iletilmesi, işlenmesi, depolanması gibi yeni alanlar ve bununla ilgili yeni teknolojiler ortaya çıkmasına neden olmuştur. Bu teknolojiler sayesinde insan yaşadığı dünyaya alternatif olan farazi (sanal) bir dünya oluşturmuştur. Bu hayali dünyanın neredeyse tamamını bugün Internet oluşturmaktadır [1].

İnternet kullanıcıların birbirlerine karşılıklı güvendiği, çalışmalarını ve edindikleri bilgileri paylaştığı akademik bir ortam olarak tasarlanmıştır. Bu araştırma tabanlı ağ ortamında kullanılmak amacıyla geliştirilen protokoller ve bu protokollere bağlı hizmetler mevcuttur. Bu protokollerden birisi TCP/IP protokolüdür. TCP/IP protokolü esasen, farklı bilgisayarlar arasında iletişim kurma görevini gerçekleştirmektedir. Bu protokol kümesi, çok sayıda yardımcı program içermektedir.

Bugünkü internet ortamının, gerçek dünyada olduğu gibi tehlikeli ve kötü niyetli kişiler tarafından da farklı amaçlar için kullanıldığını görmekteyiz. Açık bir ağ olan internet, ticari amaçlı kullanımının da yaygınlaşmasıyla, saldırıların hedef noktası olabilmektedir. Kurum ve kişiler, internet ortamına güvenlik endişesiyle girmekten kaçınabilmekte, bir yandan da böyle bir ortamda bulunmamanın büyük bir eksiklik olacağını bilmektedirler.

Alınan güvenlik önlemleri, saldırıları azaltarak sistemi saldırıların hedefi olmaktan uzaklaştırabilir ve bu saldırıları düşük maliyetli duruma getirerek sisteme ciddi zararlar vermesini engelleyebilir. Güvenlik önlemleri genel olarak bilgisayar (host) ve ağ düzeyli güvenlik önlemleri olarak adlandırılabilir. Bilgisayar (host) düzeyinde; ağdaki her bir bilgisayarın donanımına, işletim sistemine, uygulama programlarına ve sağlanan hizmetlere bağlı olarak güvenlik önlemleri alınır. Bu yöntem küçük çaplı ve çok iyi güvenlik önlemi gerektiren sistemler için idealdir.

Ağ ortamındaki bilgisayar sayısı ve çeşidi arttıkça, buna paralel olarak her bir bilgisayar sistemi üzerinde güvenlik önlemi alma işi de zorlaşır. Bu durumda ağ güvenlik modeli kullanılır. Ağ düzeyindeki güvenlik önlemleri ile ağın tamamı, ağa giriş ve çıkış noktalarında alınan önlemlerle korunmaya çalışılır. Güvenlik duvarı ile güvenlik önlemleri sistemdeki birimlere dağıtılmak yerine, ağa giriş/çıkış noktasında toplanır ve bu noktada ağa ve hizmetlere erişim kısıtlanır, izin verilen erişimler izlenerek kayıtlar tutulur.

Güvenlik duvarı mimarileri; çift taraflı geçit tipinde (dual-homed gateway host), perdelenmiş kullanıcı tipinde (screened-host) ve perdelenmiş alt ağ tipinde (screened subnet) olmak üzere üç kategoride sınıflandırılmaktadır. Bu mimariler arasındaki temel farklılık; yönlendirici ve tabya (bastion host) sayısı ve bunların ağdaki konumlarından kaynaklanmaktadır. Kurumlar bütçelerine ve güvenlik politikalarına göre güvenlik duvarı bileşenlerini uygun sayıda ve biçimde kullanarak yapılandırabilirler.

Günümüzde güvenlik duvarı oluşturabilmek ve bu sayede ağ güvenliğinin sağlanması için birçok ağ güvenlik modeli vardır. Bu modellerden birisi de ağ ortamında ISA sunucu sistemi kullanmaktır. ISA sunucular, interneti hızlandırmakla birlikte, dışardan gelebilecek saldırılara karşı ağı koruyan ve faydalı kayıtlar tutup, sistem yöneticisini uyaran çok işlevli bir yapıya sahiptir.

Güvenlik duvarlarının gerçekleştirdiği görevlerden birisi de şifrelemedir. Şifreleme, ağ ortamında gönderici ve alıcı arasında işlem gören bir bilginin, güvenli bir halde kalabilmesi için, bir takım algoritmalar kullanarak, anlaşılamaz biçime getirilmesidir. İki tür şifreleme yöntemi vardır. Bunlardan birincisi, açık anahtarlı şifreleme, ikincisi ise gizli anahtarlı şifrelemedir. Tez de uygulamaları gerçekleştirilen şifreleme algoritmaları, açık anahtarlı şifreleme yapısını kullanmaktadır. Açık anahtarlı şifreleme, birbirinden farklı iki anahtar kullanmaktadır. Bunlar genel anahtar ve özel anahtarlardır. Genel anahtar herkesçe bilindiği için bu yöntem açık anahtarlı şifreleme olarak isimlendirilmiştir. En çok tercih edilen açık anahtarlı şifreleme algoritmaları, RSA ve Eliptik Eğri algoritmalarıdır. Bu algoritmaların her birinin uygulamaya göre değişen artı ve eksileri vardır. Fakat son zamanlarda Eliptik Eğri algoritması, gerek anahtar boyutu, gerekse hız ve güvenlik olarak RSA' ya karşı üstünlük sağlamıştır.

Tez, ilk bölüm olan girişle birlikte dokuz bölümden oluşmaktadır. İkinci bölümde güvenlik konusunda genel bilgiler verilmiş ve üçüncü bölümde güvenlik stratejileri açıklanmıştır. Dördüncü bölümde güvenlik duvarı, güvenlik duvarı modelinin birimleri konuları incelenmiştir. Beşinci bölümde TCP/IP protokolü ve şifreleme, altıncı bölümde güvenlik duvarı uygulaması, yedinci bölümde RSA ve Eliptik Eğri şifreleme uygulama programı; sekizinci bölümde sonuç kısmı ve dokuzuncu bölümde ise kaynaklar kısmı bulunmaktadır.

2. GENEL BİLGİLER

Bu bölümde, bir sistemde korunması gereken hususlar açıklanmış, sisteme yönelik saldırı türleri hakkında bilgi verilmiş olup, son olarak sistemleri koruma yöntemlerinden bahsedilmiştir.

2.1. Sistemde Korunması Gereken Hususlar

İnternet'e bağlanıldığında üç şey risk alanına girer:

1. **Veriler:** Bilgisayar ortamındaki bilgiler
2. **Kaynaklar:** Bilgisayarlar
3. **Kimlik:** Kurum ya da kişi adları

2.1.1. Veriler

Veriler için önemli üç özellik şunlardır:

- **Gizlilik (Privacy) :** Bazı verilerin ve bilgilerin başkaları tarafından bilinmesi istenmez.
- **Bütünlük (Integrity) :** Verilerin başkaları tarafından değiştirilmesi ve bozulması istenmeyen bir durumdur.
- **Kullanılabilirlik (Availability):** Veri sahibinin, verilere istenildiği zaman erişip, kullanabilmesidir.

Verilerin gizliliği; örneğin, bir firmaya ait finansal kayıtlar, yeni bir ürün tasarımı ya da bir üniversitenin öğrencilerine ait bilgiler, gizlilik içermesi gereken konulardır. Bu tür önemli bilgileri internet' e bağlı olmayan daha güvenli bilgisayar sistemlerinde tutmak mümkündür. Önemli veriler internet ortamından uzak, güvenli bir bilgisayar sisteminde tutulduğunda güvenlik konusunda kaygılanmaya gerek kalmayabilir. Bütünlük ve kullanılabilirlik sorunlarının da aşılması gerekir. Ağ kullanımında amaç, verilere gizlilik ve bütünlük çerçevesi içinde, kolay erişimi ve güvenli paylaşımı sağlamaktır.

Bilgisayar ortamındaki veriler çok gizli olmasa bile, bunların değiştirilmesi, silinmesi ya da bozulması, hiç istenmeyen bir durumdur. Çünkü bu verileri yeniden elde etmek için para, zaman ve emek harcamak gerekecektir. Ayrıca; verilerin kolay ve sık bozulması, sisteme olan güveni de sarsar. Sistemlere izinsiz girilmesi durumunda bunu fark etmek ve yapılanları anlamak uzun zaman alabilir. Sisteme giren ve sistemi bozan bir olayla ilgilenmek, sisteme giren ve hiçbir şey yapmamış gibi görünen bir olayla ilgilenmekten çok daha kolaydır.

2.1.2. Kaynaklar

Bilgisayar kaynakları doğal kaynaklar değildir. Kişiler, bilgisayar sistemleri için büyük miktarlarda para, zaman harcarlar ve bunların nasıl kullanılacağını belirlemek kendi haklarıdır. Bir saldırgan (hacker), sistemdeki atıl kaynakları kolaylıkla tespit edip bunları kullanabilir ve bunun diğer kullanıcılara hiçbir ek yük getirmediğini iddia edebilir. Fakat, kullanıcı bir dizi animasyon başlattığında belleğin her bir bitine, işlemcinin her bir mikro saniyesine ihtiyaç duyar ve bu kaynaklara ihtiyaç duyduğu anda sahip olmak ister.

2.1.3. Kimlik

Sisteme giren bir saldırgan, internet' de sistem sahibinin kimliği ile yer alacaktır. Yaptığı her şey sistem sahibi tarafından yapılmış gibi olacaktır. Örneğin, bir saldırgan sisteme girerek çeşitli çevrelere kötü niyetli e-postalar gönderebilir. Böyle bir e-postaya az sayıda inanan olsa dahi, bunun etkilerini ortadan kaldırmak kişinin zamanını alacağı gibi, kimliği üzerinde kalıcı etkiler de yaratabilir. Bir sisteme giren saldırgan, bu sistem üzerinden başka kişi ya da kuruluşların sistemine girerek bu sistemlere de zarar verebilir. Bu durumda sorumlu, aracı olarak kullanılan sistem sahipleri olacaktır. Çoğu saldırganlar girdikleri siteleri korsan yazılım ve pornografik dağıtım yapan siteler olarak gösterirler. Bu tür olaylar hoş karşılanmayacağı gibi, kuruluşa da olan güveni sarsar ve etkilerini gidermek hayli güç olabilir.

2.2. Sisteme Yönelik Saldırı Türleri

Bir sisteme yapılacak saldırı türleri çok çeşitli olabilir. Farklı biçimlerde de sınıflandırılabilecek olan saldırı türleri genel olarak üç kategoride sınıflandırılır:

1. Sisteme izinsiz girme (Intrusion)
2. Hizmet kullanımını engelleme (Denial of service)
3. Bilgi hırsızlığı (Information theft)

2.2.1. Sisteme İzinsiz Girme

En sık kullanılan saldırı türüdür. Bu yolla sisteme giren saldırgan sistemin yetkili kullanıcısı gibidir. Bu tür bir saldırı için en basit yol saldırganın kendisini sisteme yetkili bir kullanıcı olarak tanıtmasıdır (false authentication). Bir başka yol ise yetkili bir kullanıcı gibi kendisini sisteme tanıtarak kurmuş olduğu bağlantıyı çalmaktır.

2.2.2. Hizmet Kullanımını Engelleme

Saldırganların seçtiği yöntemlerden bir diğeri de, saldırıda bulundukları sistemi çok sayıda mesaj ve işlem istemleri ile boğmak ve sistemin yapması gereken işi engellemektir. Bu durumda sistem bütün zamanını bu istem ve mesajları yanıtlamak için harcar. Daha akıllıca davranan saldırganlar (hacker) hizmeti tamamen engellemekte, farklı yöne yönlendirmekte ya da farklı bir hizmet ile değişmektedir. Böyle bir saldırı 1994 yılında IBM firmasına karşı gerçekleştirilmiştir. Posta ve telefon hizmetine ilişkin programlar değiştirilmiş, çok sayıda posta ile boğulan hizmet, ağ bağlantısının kapanmasına neden olmuş ve gelen telefonlar farklı bölgelere yönlendirilmiştir. Bu yöntemi eğlenceli bulmayan saldırganlar, bu tür saldırıları çok nadir olarak yapmaktadırlar. Bu tür sorunlarla, daha çok yapılan hatalardan dolayı karşılaşılmaktadır.

2.2.3. Bilgi Hırsızlığı

Bazen saldırganlar doğrudan sisteme girmeden de verilere erişebilirler. İnternet hizmeti kullanıcıya gerekenden fazla bilgi sağlayabilir. Birçok internet hizmeti yerel ağ (LAN) üzerinde kullanılmak üzere tasarlanmıştır. Bu hizmetler internet üzerinde güvenli biçimde kullanılacak derecede güvenlik önlemi içermemektedir. Bilgi hırsızlığı, pasif bir biçimde iletişim hattının dinlenmesi ile olabileceği gibi aktif bir biçimde, örneğin kişinin kendisini yetkili biri gibi tanıtıp bilgi istemesi yoluyla da olabilir.

2.3. Sisteme İzinsiz Girişler

Sistemdeki açıkları bularak sisteme izinsiz giren kişiler saldırgan (hacker) olarak adlandırılır. İnternet üzerinde çok sayıda saldırgan vardır. Bunların genel özellikleri:

- Girdikleri sistemlere daha sonra tekrar girebilmelerini sağlayacak yollar açarlar.
- Birbirleri ile iletişim kurarak, elde ettikleri bilgileri paylaşırlar.
- Yakalanmak istemezler, kendilerini gizli tutarlar.

Saldırganlar niyetlerine göre 4 gruba ayrılabilir:

- **Eğlence Arayanlar**

Bunlar sıkılmış, eğlence arayan, meraklı fakat; kötü niyetli olmayan kişilerdir. Tanınmış siteler ve bilinmeyen bilgisayarların meraklısıdırlar. Bilgisayarlardaki özel verileri okumaktan ve başkalarının bilgisayarlarını kullanmaktan zevk alırlar.

- **Kötü Niyetliler**

Bu guruba giren saldırganlar sistemi bozmayı amaçlarlar. Bozmaktan zevk alırlar ve güçlerini bu yolla göstermeye çalışırlar. Bu tür kişilerin sayıları maalesef sürekli artış göstermektedir. Ülkeler yasalarında değişiklikler yaparak, bu tür kötü niyetli kişilerle mücadele etmeye çalışmaktadır.

- **Skor Meraklıları**

Bu saldırganlar girdikleri sistemlerin sayısı ve türü ile övünürler ve bu yüzden girebildikleri bütün sistemlere girerler. Girdikleri sistemlerin bilinmesi, iyi korunması ve düzenli olması onlar için önemli özelliklerdir.

- **Casuslar**

Bu kişilerin amacı; gizli ve özel verileri elde ederek, bunları kazanç sağlamak amacıyla kullanmaktır. Saldırganlar girdikleri sistemlere daha sonrada girebilecek duruma gelmeye ve girdikleri sistemlerden başka sistemlere geçmeye çalışırlar. Sisteme giren bu kişileri fark etmek uzun zaman alabilir.

2.4. Sistemleri Koruma Yöntemleri

Kişiler ve kuruluşlar bu konuda çeşitli güvenlik modellerini tercih edebilirler. Bu modeller:

- Güvenlik önlemi almama
- Bilgisayar (host) düzeyinde güvenlik önlemi
- Ağ düzeyinde güvenlik önlemi

2.4.1. Güvenlik Önlemi Almama

En basit yaklaşım, hiçbir güvenlik önleminin alınmamasıdır. Donanım ve yazılımın sağladığı minumum düzeydeki güvenlik önlemi ile yetinmektir. Bu modelde sistemin varlığının, içeriğinin ve güvenlik önlemlerinin kimse tarafından bilinmediği düşünülerek, güvende olduğu varsayılır. Fakat bu yaklaşım uzun süre etkili olmaz, çünkü saldırganlar için etkili hedefleri bulmanın birçok yolu vardır. Bazı kişiler sistemlerine girilse bile bunun önemli olmayacağını, küçük bir şirketin ya da evdeki kişisel bir bilgisayarın saldırganın ilgisini çekmeyeceğini düşünürler. Fakat bütün saldırganlar özel hedefler aramazlar ve girebildikleri bütün sistemlere

girerler. Küçük bir şirket ya da evdeki bir bilgisayar onlar için basit ve kolay bir hedeftir. Bu tür sistemlerde uzun süre kalmazlar, fakat yazılımlara ciddi zararlar verebilirler. Sistemin donanımı, üzerindeki yazılımlar, işletim sistemi ve sürümü saldırganlara güvenlik açıkları konusunda önemli bilgiler verir.

2.4.2. Bilgisayar (host) Düzeyinde Güvenlik Önlemi

En yaygın olan modeldir. Her bir bilgisayar (host) üzerinde bütün güvenlik açıklarına karşı önlemler alınır. Modelin uygulanmasındaki en büyük sorun, sistemlerin karmaşıklığı ve farklılığıdır. Büyük bir yerel ağda, çok sayıda farklı bilgisayar sistemi, bu bilgisayarlar üzerinde farklı işletim sistemleri, aynı işletim sisteminin farklı sürümleri, farklı uygulama programları ve dolayısıyla her bir bilgisayarda birbirinden farklı güvenlik problemleri olabilir. Bu modelin devamlılığını sağlama, devamlı olarak sistem üzerinde gerekli değişikleri yapmayı gerektirir.

Model, küçük çaplı ve çok iyi güvenlik önlemi gerektiren sistemler için idealdir. Ayrıca her sistem genel güvenlik önlemi bağlamında belirli düzeyde bilgisayar (host) güvenliği de içermelidir. Bilgisayar (host) güvenliği, maliyetin yüksek olması nedeniyle, ancak küçük ve basit sistemler için uygulanabilir.

2.4.3. Ağ Düzeyinde Güvenlik Önlemi

Ağ ortamındaki bilgisayar sayısı ve çeşidi arttıkça, buna paralel olarak her bir bilgisayar (host) üzerinde güvenlik önlemi alma işi de zorlaşır. Bu durumda ağ güvenlik modeli kullanılır. Bu modelde yerel ağı korumak için güvenlik duvarı oluşturulur, daha güçlü kimlik denetleme yöntemleri kullanılır ve veriler internet üzerinden gönderilirken şifrelenir. Bilgisayar (host) güvenliğinde de belirtildiği gibi ağ güvenlik modeli kullanılsa bile, çok önemli bilgilerin tutulduğu ve internet'e doğrudan bağlı olan bilgisayarlar için bilgisayar (host) güvenlik modeli uygulanmalıdır. Ayrıca bilgisayarları yerel ağdan gelecek tehlikelere karşı korumak için de yine bilgisayar (host) güvenlik modeli gereklidir.

Her türlü önleme rağmen bütün problemleri çözecek genel bir güvenlik modeli yoktur. Örneğin; yetkili bir kullanıcı sisteme bilinçli olarak zarar verebilir ya da sisteme fiziksel olarak zarar verilebileceği gibi bilgi, farklı ortamlarda ağ dışına taşınabilir. Sorunların bir kısmı da yapılan hatalardan kaynaklanmaktadır. Güvenlik olayları konusunda yapılan bir araştırma, olayların %55'nin tecrübesizlik ve bilgisizlikten kaynaklandığını ortaya koymuştur. Kuruluşlar yanlışlıkla verilerini silebilmekte ya da başkalarının erişimine açabilmektedirler. Sistemi kötü niyetli kişilere karşı koruduğumuzda, hatalara karşı da korumuş oluruz. Alınan güvenlik

önlemleri sisteme yapılan saldırıları azaltır, düşük maliyetli duruma getirir ve sisteme ciddi zararlar verilmesini engeller.

Ülkemizde İnternet'in yaygın biçimde günden güne kullanılmasının artması, olumlu bir gelişme olarak değerlendirilirken, bu iletişim aracının bazı olumsuz gelişmelere de sebep olduğu bilinmektedir. İnternet kullanımının hızlı yaygınlaştığı bir süreçte, İnternet aracılığı ile işlenen çeşitli suçlar karşısında yeterli yasal düzenlemelere sahip olduğumuzu söylemek mümkün değildir.

Bilişim teknolojileri; yazılım telif hakları, Türk Hukukunda fikir ve sanat eserlerini koruma ve etik sorunlarını beraberinde getirmiştir. Bilişim suçlarına karşı çeşitli mücadele teknikleri geliştirilmeye çalışılmaktadır. Bu bağlamda "Bilgisayar ve Bilgisayar Şebekeleri ile İlgili Türk Ceza Kanunu'nda" değişiklikler önerilmektedir.

Bilişim ortamında kişilere özel bilgilerin korunması, kişilerin kamusal makamlarda ve özel kuruluşlar nezdindeki bilgilerin tutulacağı veri taban dosyaları ve içeriklerinin kapsamı konusunda hangi sınırların dışına çıkıldığında suç işlendiği varsayılacağı, belirsizlik olarak karşımıza çıkmaktadır [2].

Bilimsel teknolojilerin toplum üzerinde olumlu ve olumsuz birçok etki yapacağı gerçeği göz önüne alındığında, kısa süre içerisinde özellikle olumsuz gelişmelere çözüm bulabilecek yasal düzenlemelerin yapılması gerekir. Hukuksal boyuttan bakıldığında, çıkarılacak yasal düzenlemelerin sadece günün şartlarında ortaya çıkabilecek bilişim suçlarını bertaraf etmeyip, geleceğe yönelik teknolojilere de cevap verebilir nitelikler taşıması gerekir.

3. GÜVENLİK STRATEJİLERİ

3.1. Kısıtlı Yetki

Kısıtlı Yetki, en temel güvenlik stratejisidir. Sistemdeki her birim (sistem yöneticileri, kullanıcıları, programlar) yalnızca yapması gereken işi yapacak kadar gerekli yetkiye sahip olmalıdır.

Bu konuda internet ortamında birçok örnek vardır:

- Bütün kullanıcıların tüm hizmetlere erişme ihtiyacı yoktur.
- Bütün kullanıcılar, sistemdeki tüm dosyaları okuma/yazma gereksinimi duymaz.
- Bütün kullanıcıların root şifresini bilmesi gerekmez.
- Bütün sistem yöneticilerinin her bir bilgisayarın root şifresini bilmesi gerekmez.

Kısıtlı yetkinin tam olarak uygulanmaması, güvenlik problemlerine neden olmaktadır. Örneğin, posta gönder (send mail) büyük ve karışık bir programdır. Bu programın görevini yapması için sistemde root olarak çalışması gerekir. Büyük ve karmaşık olması ve sistemde root olarak çalışması nedeniyle, güvenlik açıkları olan bir programdır. Bu tür programları yazarken, özel yetki gerektiren kısımları, diğer kısımlardan ayırmak gerekir.

Kısıtlı yetkiyi uygulamada iki problemle karşılaşılır:

- Eğer kullanılan program ya da protokol kısıtlı yetkiye olanak vermiyorsa, gerçekleştirim güçleşir.
- Sistemdeki birimlere gerekenden daha az ya da daha çok yetki verilebilir.

Sistemdeki kullanıcılara işlerini yapması için gerekli yetkiyi vermek gerekir. İnsanlar yapmak istedikleri işleri yapamayınca sinirlenirler. Sistem için kendi kullanıcılarını sinirlendiren bir durum oluşturmamak gerekir.

3.2. Çok Düzeyli Savunma

Bir diğer güvenlik stratejisi de çok düzeyli savunmadır. Çok düzeyli savunmada birbirini destekleyen birden çok güvenlik önlemi alınır. Yani; güvenlik önlemlerinden birini aşan saldırgan bir diğeri ile karşılaşır. Amaç; saldırganın işini daha zor ve riskli hale getirmektir. Bu da ağ güvenliği, bilgisayar (host) güvenliği, kişisel güvenlik önlemleri gibi bir dizi güvenlik mekanizması ile sağlanabilir. Bunlardan yalnızca birine güvenmemek gerekir, her biri önemli ve etkili güvenlik mekanizmasıdır.

3.3. Boğum Noktası

Boğum noktası, sisteme girmeye çalışanları denetlenen dar bir kanalı kullanmaya zorlar. Bu yöntemin gerçek hayatta birçok örneği vardır. Kütüphanelere, marketlere ve sinemalara giriş ve çıkışların belirli noktalardan sağlanması bu duruma örnek verilebilir. Ağ güvenliği bağlamında da güvenlik duvarı bir boğum noktasıdır. Sisteme dışardan girmek isteyen kişiler, bu noktayı kullanmak zorundadır. Bu noktada gerekli güvenlik önlemleri alınarak yetkisiz kişilerin ağa girişi engellenir. Eğer sisteme başka noktalardan da giriliyorsa, boğum noktası kullanışlı bir yöntem olmaz. Sisteme çevirmeli hatlar (dial-up) kullanılarak girilebiliyorsa, saldırgan güvenlik duvarı üzerinden girmek yerine bu yolu tercih eder. Boğum noktası, bütün yumurtaları bir sepete koymaya benzetilmektedir. Fakat bunun iyi korunan bir sepet olduğu da bilinmelidir. Dikkati sistemdeki birimler üzerinde oluşacak sorunlara dağıtmak yerine, tek bir noktada yoğunlaştırmak daha anlamlıdır.

3.4. Zayıf Nokta

Bir zincir en zayıf halkası kadar, bir duvar en zayıf noktası kadar güçlüdür. Bu görüş bilgisayar sistemleri için de geçerlidir. Saldırganlar sistemdeki zayıf noktaları bulup, bu noktalardan sisteme girmeye çalışırlar. Sistemin zayıf noktalarının belirlenip, bu noktalarda gerekli önlemlerin alınması ya da en azından bu noktaların izlenmesi gerekir. Her zaman zayıf bir nokta bulunacaktır. Amaç; bu noktayı mümkün olduğunca güçlü tutmaktır.

3.5. Başarısızlık Durumunda Güvende Kalmak

Bütün sistemler bir sorun oluştuğunda işleyişlerini güvenli bir biçimde sonlandırmayı amaçlar. Bilgisayar sistemlerinde de güvenlik birimlerinde bir sorun oluştuğunda saldırganların sisteme girişi engellenmelidir. Sistem başarısızlık durumunda yetkili kişilerin de girişini engeller, fakat bu kabul edilebilir bir kısıtlamadır. Örneğin, filtreleme yapan yönlendiricide bir sorun oluşmuş ise bütün paketler filtrelenmeli ya da bir vekil (proxy) sunucusunda sorun çıktığında ilgili hizmet engellenmelidir.

Bu stratejide uygulanabilecek iki tür güvenlik politikası vardır:

1) Kesin olarak izin verilenler dışında her şeyi engellemek
2) Kesin olarak engellenenler dışında her şeye izin vermek

1) Kesin olarak izin verilenler dışında her şeyi engellemek

Bu yöntemle kesin olarak izin verilmeyen her şey engellenir. Bilinmeyen kişilerin sisteme girmesine, bilinmeyen işlemlerin yapılmasına izin verilmez. Uygulamada önce her şey engellenir, daha sonra nelere izin verileceği kararlaştırılır. Bunun için;

- Kullanıcılar için gerekli hizmetler belirlenir.
- Bu hizmetlerin güvenlik sorunları incelenir ve güvenli biçimde sağlamanın yolları araştırılır.
- Yalnızca işlevi bilinen ve güvenli biçimde sağlanabilecek olan hizmetlere izin verilir.

2) Kesin olarak engellenenler dışında her şeye izin vermek

Bu yöntemde kesin olarak engellenmeyen her şeye izin verilir. Kullanıcı ve yöneticiler bu politikayı tercih ederler. Çünkü onların düşüncesine göre her şeye izin verilmeli, yalnızca sorunlu hizmetler engellenmelidir. Bu politikaya göre tehlikelerin ve bunlara karşı nasıl korunacağının bilindiği varsayılır. Fakat bu imkansızdır, çünkü sistemlerde zamanla yeni güvenlik açıkları ortaya çıkmaktadır. Bu yöntemde sorun olduğu bilinmeyen şeyler engellenemez.

3.6. Savunmada Çeşitlilik

Farklı türde sistemler kullanmak güvenlik önlemini arttırır. Eğer bir ağ ortamındaki bütün sistemler aynı türden ise, birine erişmeyi başaran saldırgan, diğerlerine de benzer biçimde ulaşabilir. Bu güvenlik stratejisinin arkasındaki temel düşünce, eğer sistemler farklı üreticilerden alınırsa, sistemin kendisinden ya da konfügürasyonundan kaynaklanan hatalardan bütün sistem etkilenmez. Bu stratejide hayali farklılıktan kaçınmak gerekir. Örneğin, farklı satıcılardan UNIX işletim sistemi almak, sisteme farklılık getirmez. Çünkü çoğu UNIX işletim sistemi BSD (Berkeley Software Distribution) ya da System V kaynak kodundan türetilmiştir.

Aynı kişinin konfügürasyonunu yaptığı sistemlere de dikkat etmek gerekir. Sorun teknik düzeyde değil, kavramsal düzeyde olabilir. Bu yöntemin dezavantajı, karmaşıklık ve maliyettir. Kuruluşlar farklı türden sistemler kullanmanın güvenliği arttırdığını onaylamaktalar, fakat maliyet ve diğer problemler, güvenlikteki gelişmeyi karşılamamaktadır.

3.7. Basitlik

Sistemlerin ve programların karmaşıklığı arttıkça, denetimleri güçleşir. Basitlik anlaşılırlığı arttırır ve sistemdeki değişikliklerin kolay fark edilmesini sağlar. Ayrıca, basitlik saldırganların sistem içerisinde gizlenmesini de güçleştirir. Karmaşık programlar daha çok hata içerir. Hataların kendisi güvenlik problemi olmasa bile, kullanıcılar sistemin düzensiz çalıştığını düşünmeye başlayınca, her şeyin olabileceğini kabul ederler ve güvenlik konusundaki titizliklerini yitirirler.

3.8. Genel Katılım

Güvenlik sisteminin tam ve etkili olması, genel katılımı gerektirir. Katılım; isteyerek ya da kural gereği olabilir. Kullanıcılar; güvenlik konusunda eğitilerek, katılımın isteyerek olması sağlanmalıdır. Sistem yöneticisi ya da güvenlikten sorumlu kişi her şeyi kontrol edemez.

Kullanıcıların da karşılaştıkları farklı durumları sistem yöneticisine bildirmesi gerekir. Ayrıca kullanıcılar şifre seçiminde titiz davranmalı ve şifrelerini periyodik olarak değiştirmelidirler.

Kurumlar; ihtiyaç duydukları güvenlik düzeyine ve mali güçlerine göre çeşitli güvenlik stratejilerinden bir ya da birkaçını seçerler. Fakat, bu stratejilerden her biri ağ güvenliği için çok önemlidir. Bunlardan yalnız bir ya da ikisine bağlı kalmak yerine her birinin belirli düzeyde gerçekleştirilmesi gerekir. Özetle, titiz bir çalışma gerektiren ağ güvenliğinde yetkiler uygun bir biçimde dağıtılmalı, ağa giriş ve çıkış noktasında trafik denetlenmeli, sistemin yalınlığına dikkat edilmeli, sistemdeki açıklar kontrol edilerek önlemler alınmalı, kullanıcılar eğitilmeli ve çeşitli düzeylerde kullanılacak yazılım ve donanım nitelikli kaynaklarla ağın güvenliği sağlanmaya çalışılmalıdır.

4. GÜVENLİK DUVARI

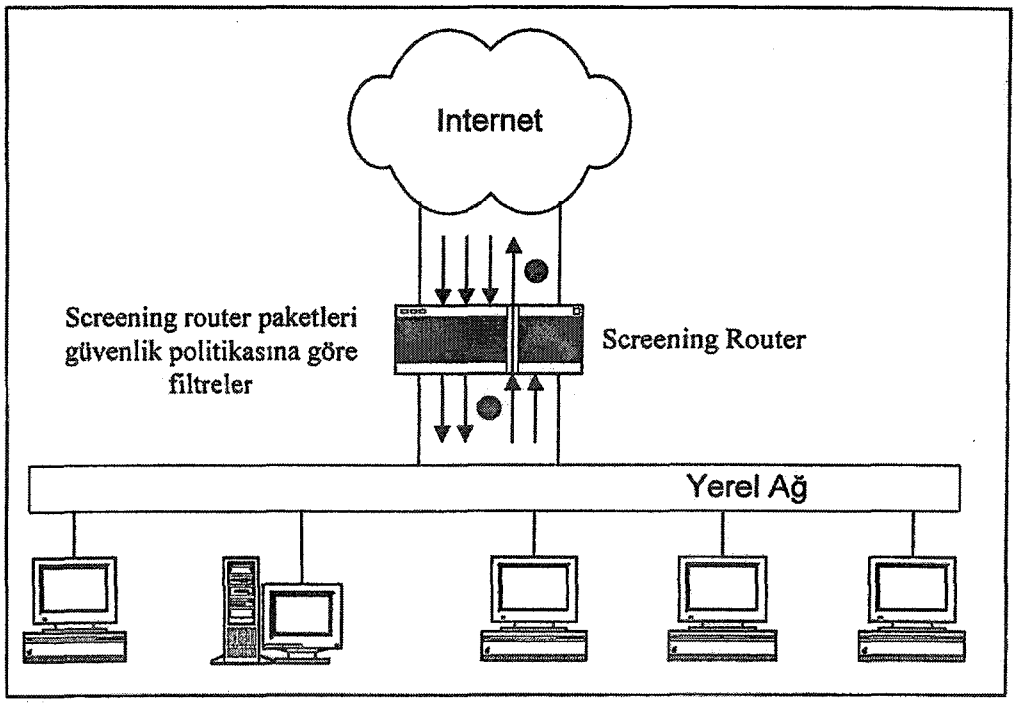
4.1. Güvenlik Duvarı

Genel bir tanımla güvenlik duvarı, yerel ağı internet ortamından gelebilecek tehlikelere karşı koruyan ağ güvenlik modelidir. Daha geniş bir tanımla, ağa giriş ve çıkışları bir noktadan sağlayarak, ağ trafiğinin kontrolünü kolaylaştıran, güvenlik önlemlerini sistemdeki birimlere dağıtmak yerine, bir noktada toplayan ve ağ aktiviteleri konusunda verimli kayıtlar tutulmasını sağlayan etkin bir ağ modelidir. Güvenlik duvarı ile ilgili bazı terimler şunlardır:

Bilgisayar (Host) : Ağ' a bağlı bir bilgisayar sistemidir.
Tabya (Bastion Host) : Ağ' ın internet ortamından görünen tek bilgisayar sistemidir. Bazı internet ve vekil (proxy) hizmetleri bu bilgisayar tarafından sağlanır.
Çift Taraflı Bilgisayar (Dual-Homed Host) : En az iki ağ ara yüzüne sahip bilgisayar sistemidir.
Paket : İletişimde kullanılan temel veri birimidir.
Paket filtreleme: Bir paketin bir ağdan diğerine gönderilirken engellenmesi ya da yönlendirilmesidir. Bu işlem tanımlanan bir dizi kural ile gerçekleştirilir ve tarama (screening) olarak adlandırılır.
Perimeter Ağ : Korunan yerel ağ ile internet arasına ek bir güvenlik önlemi sağlamak amacıyla eklenen ağdır. Bu ağ DMZ (Demilitarized Zone) olarak da adlandırılır.
Proxy sunucusu : Güvenlik duvarı (firewall) mimarilerinde istemci ile sunucu arasındaki iletişimi sağlayan ve bu iletişimi izleyen ve sınırlandıran programlardır. Güvenlik duvarı oluşturmak için kullanılan en yaygın yaklaşım, paket filtreleme ve vekil (proxy) sunucularının birlikte kullanılmasıdır.

4.1.1. Paket Filtreleme

Paket filtreleme sistemleri; ağı internet ortamına bağlayan yönlendiriciler üzerinde tanımlanan kurallar ile oluşturulur. Paket filtreleme sisteminde paketler, güvenlik politikasına göre oluşturulan kurallara göre engellenir ya da yönlendirilir. Filtreleme işlemi tarama (screening), filtrelemeyi yapan yönlendiriciler de tarama yönlendirici (screening router) olarak adlandırılır (Şekil 4.1.).



Şekil 4.1. Paket Filtreleme [3]

Her paket belirli bilgileri içeren başlık (header) kümesine sahiptir. Bu bilgilerden bazıları, kaynak ve hedef IP adresi, protokol türü (TCP, UDP, ICMP), TCP ya da UDP port numaraları ve ICMP mesaj türüdür. Paket filtreleme kuralları protokol başlıklarında bulunan bu bilgiler kullanılarak tanımlanır. İnternet hizmeti sağlayan sunucular belirli port numaralarında oturduğu için, yönlendiriciler belirli hizmetleri port numarasına bakarak engelleyebilir. Örneğin, internet üzerinden telnet hizmeti sağlanmak istenmiyorsa, bu hizmete (hedef port=23) gelen paketlerin engellenmesi yeterli olur.

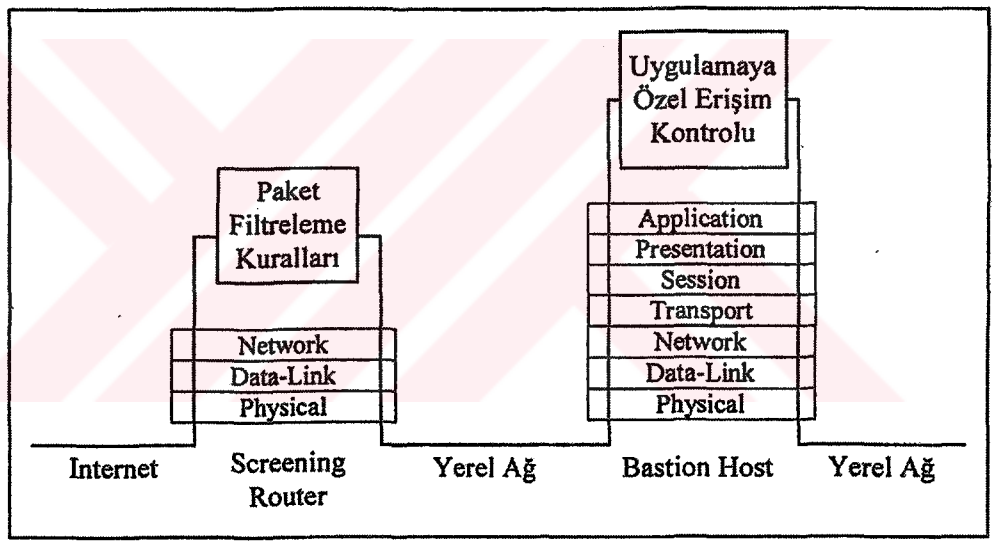
Paket filtreleme sistemlerinde internet ile yerel ağ arasında bulunan tarama yönlendiricinin (screening router) büyük sorumluluğu vardır. Eğer yönlendiricide bir sorun çıkarsa yerel ağ internet'e tamamen açık hale gelir. Ayrıca yönlendirici, bir hizmete izin verir ya da engeller, hizmetin kendisinden kaynaklanan sorunlara bir çözüm getirmez.

4.1.2. Vekil Sunucular

Bu sunucular; tabya (bastion host) üzerinde çalışan özel uygulama ya da sunucu programlarıdır. Vekil sunucuları, istemci ile gerçek sunucu arasında şeffaf bir yapıda yer alırlar. İstemci ve gerçek sunucu birbirleri ile doğrudan değil, vekil sunucusu aracılığıyla iletişim kurar. Bu sunucular kullanıcılardan gelen istemi, eğer güvenlik politikasına uygunsa, gerçek sunucuya iletirler.

Uygulama-seviyesi geçit yolu (application-level gateway) olarak da adlandırılan vekil (proxy) sunucuları güvenlik duvarı mimarilerinin her birinde kullanılabilir. Vekil (proxy) sunucusu iki bileşenden oluşur; bunlar vekil sunucusu ve vekil istemcisidir. Bileşenlerden vekil (proxy) sunucusu, tabya (bastion host) üzerinde çalışır. Vekil istemcisi ise; normal istemci programının özel bir versiyonudur. Normal istemci programı da, istemi öncelikle vekil sunucusuna yönlendirmek şartıyla kullanılabilir, fakat bu durumda vekil (proxy) sunucusu şeffaflığını yitirir.

Vekil sunucusu, bağlantı istemlerini inceler, gerekli denetimleri yapar ve bağlantıya izin verilip verilmeyeceğine karar verir. İzin verilen istemler için gerçek sunucu ile iletişim kurar ve istemci ile gerçek sunucu arasındaki istem ve yanıtları gerekli kayıtları da (log) tutarak yönlendirir. Vekil (proxy) sunucusu; yalnızca yönlendirme işlemini yapmaz, kullanıcının yaptığı işlemleri de izler. Bir hizmetteki bazı işlemlere, güvenlik politikası nedeniyle izin verilmeyebilir [3].



Şekil 4.2. Paket Filtreleme ve Vekil (Proxy) Sunucularının Çalışma Düzeyi [3]

Örneğin; bir FTP vekil sunucusu kullanıcıların yerel ağdan dışarı dosya göndermesini engelleyip, yalnızca belirli güvenilir sitelerden dosya kopyalamasına izin verebilir. Ayrıca; daha öncelikli vekil (proxy) sunucuları farklı kullanıcılar ve bilgisayarlar için farklı kısıtlamalar getirebilir.

Günümüzde istemci/sunucu programları; proxying yeteneğini de içerecek biçimde geliştirilmektedir. Şekil 4.2.' de paket filtreleme ve vekil sunucularının OSI referans modeline göre çalışma düzeyleri gösterilmiştir [3].

4.2. Güvenlik Duvarı Mimarileri

Bazı hizmetler paket filtreleme, bazıları da vekil sunucusu kullanılarak güvenli biçimde sağlanabilir. Güvenlik duvarı mimarilerinde bu iki yaklaşım genellikle birlikte kullanılır.

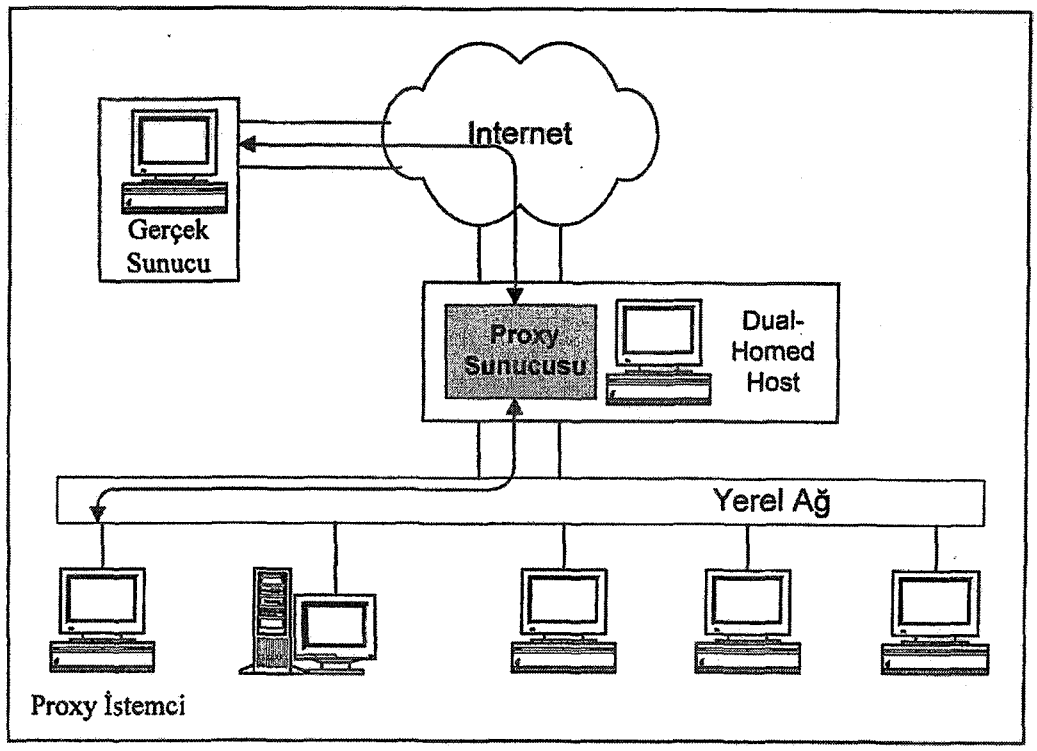
4.2.1. Çift Taraflı Geçit Tipi (Dual-Homed Gateway Host) Mimari

Bu mimaride; en az iki ağ ara yüzü olan çift taraflı bilgisayar (dual-homed host) kullanılır (Şekil 4.3.). Bu bilgisayar (host), ağ ara yüzleri arasında paket yönlendirme yapabilir.

Bu mimaride bir güvenlik duvarı oluştururken, IP paketlerinin yönlendirme özelliğinin iptal edilmesi gerekir. Örneğin, Unix işletim siteminde bu işlem, çekirdek konfigürasyonundaki IPFORWARDING parametresi –1 yapılarak sağlanır. Bu mimaride; yerel ağdaki ve internet ortamındaki bilgisayarlar birbirleri ile doğrudan iletişim kuramazlar, yalnızca çift taraflı bilgisayar (dual-homed host) ile iletişim kurabilirler.

Çift taraflı bilgisayar (dual-homed host), bu makineye login olmak suretiyle ya da bu makine üzerindeki vekil (proxy) sunucular kullanılarak internet hizmetlerinden yararlanma olanağı sağlar. Birinci durum tercih edilmez, çünkü, bu durum sistemi şifre kırma (password cracking) saldırılarına karşı açık hale getirir.

Kullanıcılar; çift taraflı bilgisayar (dual-homed host) makinesine bağlanarak; hizmetlerden yararlanmayı kısıtlayıcı bulurlar. Çift taraflı bilgisayar (dual-homed host); hem yönlendirici, hem de vekil (proxy) hizmeti sunan tabya (bastion host) görevini yapmaktadır. Bu makinenin güvenliğini sağlamak için alınacak önlemler, bir tabya (bastion host) makinenin güvenliğini sağlamak için alınması gereken önlemlerden ibarettir. Bu mimarinin dezavantajı, IP paketlerinin yönlendirme özelliği ile güvensiz hizmetlerin aktif hale getirilmesi durumunda, saldırganların ağa erişimine olanak vermesidir.



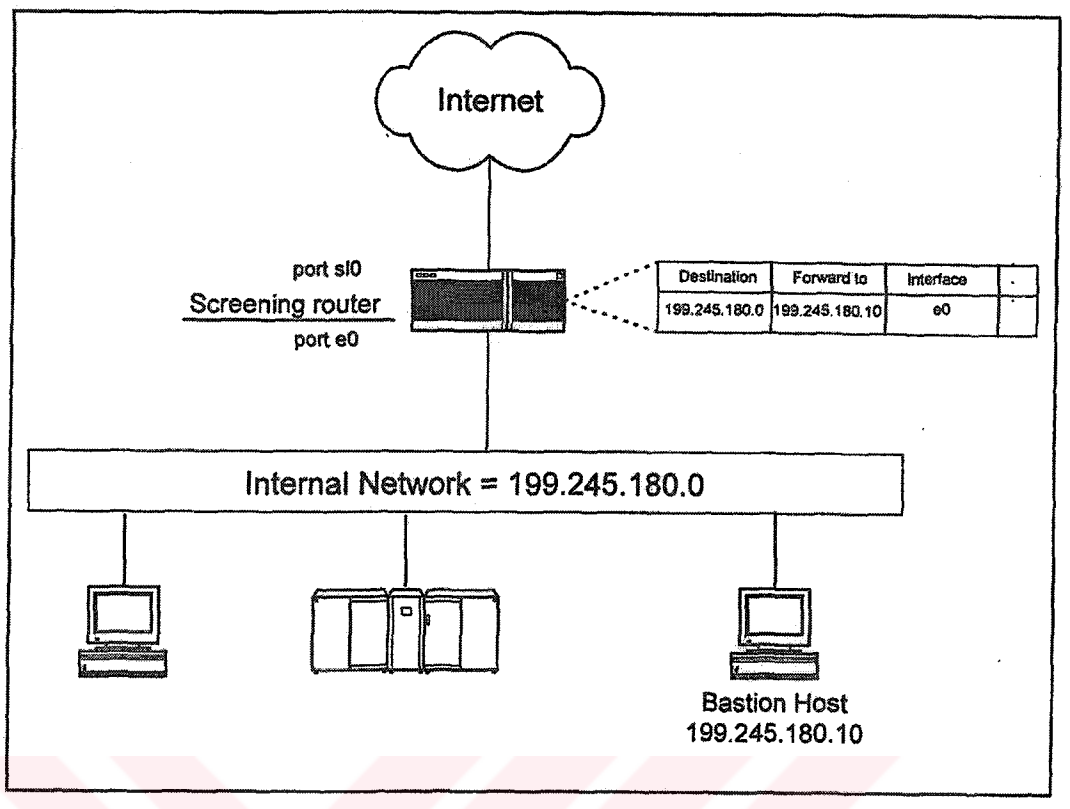
Şekil 4.3. Çift Taraflı Geçit (Dual-homed gateway host) Mimarisi [3]

4.2.2. Perdelenmiş Kullanıcı (Screened Host) Tipi Mimari

Bu mimaride; tarama yönlendiricisi (screening router) ve tabya (bastion host) birlikte kullanılır (Şekil 4.4.). Hizmetler, yerel ağa bağlı tabya (bastion host) tarafından sağlanır. Birincil güvenlik yönlendirici tarafından, paket filtreleme sistemiyle sağlanır ve vekil (proxy) sunucusunun atlatılarak, yerel ağa erişilmesi engellenir.

İnternet'ten yerel ağa erişmek ya da bir hizmetten yararlanmak isteyen kullanıcılar, öncelikle tabya (bastion host) ile iletişim kurmalıdır. Geçerli bağlantılar için tabya (bastion host), hizmeti doğrudan kendisi sağlar ya da yerel ağda, hizmeti sağlayan sunucu ile iletişim kurar.

Tabya (bastion host) saldırılara maruz kalacağı için, host güvenliği ile sıkı bir biçimde korunmalıdır. Tarama yönlendiricisi (screening router) iki farklı biçimde konfigüre edilebilir, yerel ağdaki bilgisayarların (hostların), internet ile doğrudan bağlantı kurması sağlanabilir ya da tabya (bastion host) dışındaki bilgisayarların internet bağlantısı kurması engellenerek, kurulacak bütün bağlantıların tabya üzerinden yapılması sağlanabilir.



Şekil 4.4. Perdelenmiş Kullanıcı (Screened host) Tipi Mimari [3]

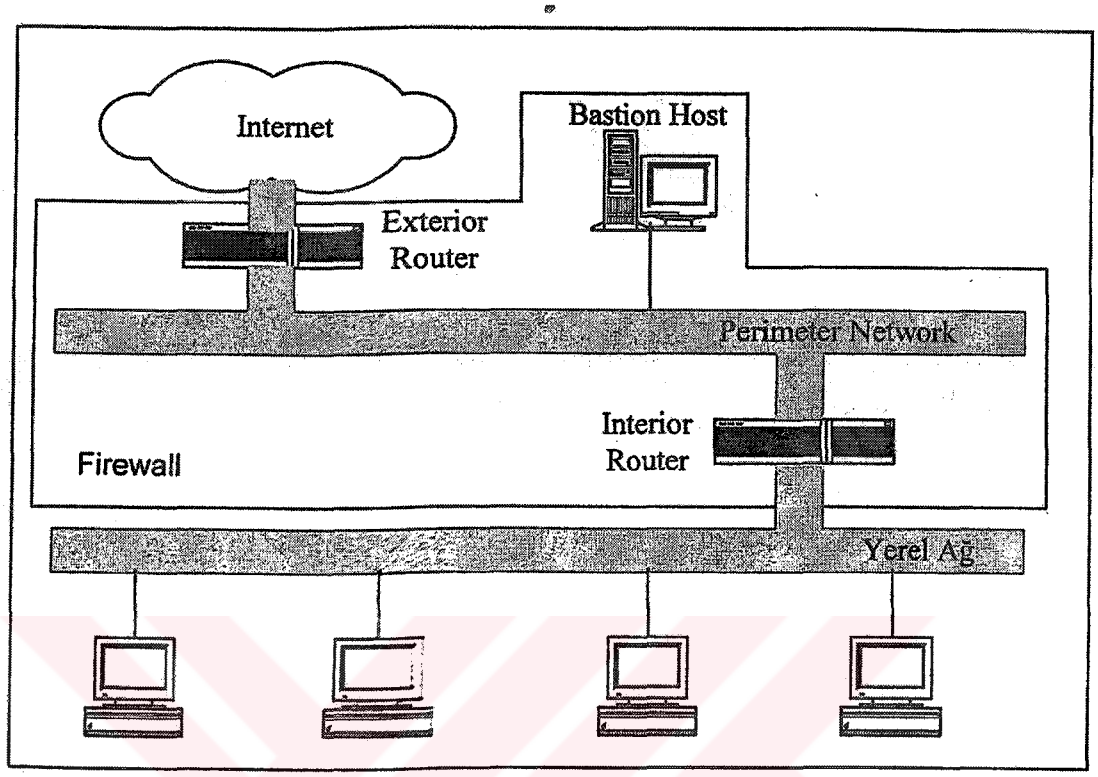
Bu mimari, paketlerin yerel ağa girmesine izin verdiği için çift taraflı bilgisayar (dual-homed host) mimarisine göre daha riskli görülebilir. Fakat bir yönlendiriciyi korumak bir bilgisayarı korumaktan daha kolaydır. Çift taraflı bilgisayar (dual-homed host), sıkı bir bilgisayar (host) güvenliği gerektirir ve konfügürasyonunda yapılacak bir hata saldırganların yerel ağa erişimine olanak verir. Sonuç olarak; perdelenmiş kullanıcı (screened-host) tipi mimari, çift taraflı bilgisayar (dual-homed host) mimarisinden daha kullanışlı ve güvenilir bir mimaridir [3].

Bu mimaride; tabya makinesine ulaşan bir saldırganın diğer bilgisayarlara ulaşmasını engelleyecek bir güvenlik önlemi yoktur. Ayrıca, yönlendiricinin konfügürasyonunda yapılacak bir hata, yerel ağı internet ortamına tamamen açık hale getirebilir.

4.2.3. Perdelenmiş Alt Ağ (Screened subnet) Tipi Mimari

Bu mimaride; yerel ağ ile internet arasına yeni bir ağ eklenerek, ek güvenlik önlemi sağlamaya çalışılır (Şekil 4.5.) [3]. Konumlarından dolayı tabya (bastion host) makineleri en çok tehlikeye maruz kalabilecek bilgisayarlardır. Perdelenmiş kullanıcı (screened host) mimarisinde, tabya (bastion host) ile yerel ağ arasında başka güvenlik önlemi olmadığı için,

tabya makinasına erişmeyi başaran bir saldırganın diğer birimlere erişmek için önünde engel kalmamış olur.



Şekil 4.5. Perdelenmiş Alt Ağ (screened subnet) Tipi Mimari [3]

Bu yüzden tabya (bastion host), perimeter ağ (network) kullanılarak yerel ağdan izole edilir ve bu makineye erişim, bütün sisteme erişime olanak vermez. Perdelenmiş alt ağ (screened subnet) mimarisi, perimeter ağ ve buna bağlı iki yönlendirici ve tabya (bastion host) makinesinden oluşur. Bu mimari de yerel ağa ulaşmak için yalnız bir bileşeni geçmek yetmez [3].

Güvenilmeyen, tehlikeye maruz kalabilecek hizmetler, dıştaki perimeter ağ üzerinden sağlanır. Yine bu mimaride; katmanlı yapının etkili olabilmesi için, her katmandaki güvenlik önlemlerinin farklı olması gerekir. Bu tür mimariler ile çok düzeyli savunma, savunmada çeşitlilik ve boğum noktası güvenlik stratejileri birlikte uygulanmış olur.

Perimeter Ağ : Bu ağ (network), yerel ağ ile internet arasında ek bir güvenlik sağlamak amacıyla kurulur. Birçok ağ yapısında her bir bilgisayarın yerel ağ trafiğini görme şansı vardır. Örneğin, çok yaygın olarak kullanılan Ethernet, Token-ring ve FDDI yerel ağlarında bu olanak vardır. Bu özellik; yerel ağdaki bir bilgisayarın ağ trafiğini dinlemesine olanak verir. Örneğin, e-postalar okunabilir ve şifreler öğrenilebilir. Perimeter ağ üzerinde yer alan tabya (bastion host)

makinesine ulaşan bir saldırgan, yalnızca bu ağ üzerindeki trafiği izleyebilir. Bu ağdaki trafik de internet ile yerel ağ arasındaki trafikten ibarettir. Yani, tabya (bastion host) makinesine erişilse de yerel ağdaki trafik güvendedir.

Tabya (Bastion Host) : Perimeter ağ (network) üzerindeki bilgisayarlar, tabya (bastion host) olarak adlandırılır ve internet üzerinden gelen iletişim istekleri bu bilgisayarlar tarafından ele alınır. Yerel ağdaki kullanıcıların internet ortamındaki hizmetlerden yararlanmaları şu şekilde olabilir:

- Yönlendiriciler üzerinde tanımlanan (exterior ve interior router) paket filtreleme kuralları ile doğrudan erişim
- Tabya (bastion host) üzerindeki vekil (proxy) sunucularını kullanarak dolaylı erişim

Dahili Yönlendirici (Interior Router) : Bu yönlendiriciler boğum yönlendirici (choke router) olarak da adlandırılır. Paketlerin büyük çoğunluğu bu yönlendirici tarafından filtrelenir.

Yönlendiricinin tabya (bastion host) ile yerel ağ ve yerel ağ ile internet arasında izin verdiği hizmetler aynı olmak zorunda değildir. Tabya ile yerel ağ arasındaki hizmetlerin kısıtlanma sebebi, bu bilgisayar (host) üzerinden ağa gelecek tehlikeleri önlemektir. Tabya ile yerel ağ arasındaki hizmetler, çok gerekli olanlarla sınırlandırılmalıdır (SMTP, DNS gibi). Ayrıca, tabya (bastion host) yalnızca hizmeti sağlayan yerel bilgisayarlarla iletişim kurmalı ve bu bilgisayarlar üzerinde gerekli güvenlik önlemleri alınmalıdır.

Harici Yönlendirici (Exterior Router) : Bu yönlendirici teorik olarak, perimeter ağ ve yerel ağı internet üzerinden gelecek tehlikelere karşı korur. Uygulamada ise; yerel ağdan gelen paketlerin geçişine izin verir ve internet üzerinden gelen paketlerin çok azını engeller. Bu yönlendiricideki filtreleme kuralları perimeter ağ üzerindeki bilgisayarları korumaya yöneliktir.

Bu bilgisayarların da çok fazla korunmaya ihtiyaçları yoktur, çünkü kendileri bilgisayar (host) güvenliği ile korunurlar. Yönlendirici, internet üzerinden gelen ve yerel ağdaki bir bilgisayarın adresini taklit eden paketleri engeller. Bu görev; dahili yönlendirici (interior router) tarafından da yerine getirilir, fakat dahili yönlendirici, perimeter ağ üzerindeki bilgisayarlardan geldiğini iddia eden paketleri engelleyemez.

Kurumlar, bütçelerine ve güvenlik politikalarına göre güvenlik duvarı bileşenlerini uygun biçimde kullanıp konfigüre edebilirler. Örneğin, mimaride birden çok perimeter ağ, bu ağ (network) üzerinde birden çok tabya bulunabilir. Kurumlar performansı artırmak, verileri ve sunucuları birbirinden ayırmak ve artıklık sağlamak için birden çok tabya (bastion host) kullanabilir.

Üçüncü nesil güvenlik duvarı olarak adlandırılan ve paket filtreleme ile vekil sunucularını birleştiren güvenlik duvarı mimarileri de geliştirilmektedir. İstemci/sunucu uygulamaları proxying özelliğini destekleyecek biçimde geliştirilirken (www istemcileri gibi) paket filtreleme sistemleri de daha esnek bir yapıya kavuşturulmaktadır. Yönlendiricinin paket filtreleme kuralları, dinamik olarak değiştirilmektedir. Örneğin, yerel ağdan giden UDP istem paketleri için geçici bir filtreleme kuralı oluşturularak, yalnızca bu isteğe cevap alan UDP paketlerinin yerel ağa girmesine izin verilir.

4.3. Güvenlik Duvarı Modelinin Özellikleri

4.3.1. Güvenlik Duvarı Tarafından Sağlanan Olanaklar

1. Güvenlik duvarı, güvenlik konusundaki kararlar için bir odak noktasıdır. Güvenlik önlemlerinin ve teknolojinin birçok birim üzerine dağıtılması yerine, bir nokta üzerinde yoğunlaştırılmasını sağlar. Güvenlik duvarı kurmanın maliyeti yüksek olmasına karşın, yine de kuruluşlar bu yöntemi diğer güvenlik önlemlerine tercih etmektedirler. Çünkü, sisteme verilen zararı karşılamanın maliyeti, güvenlik önlemleri için yapılan harcamadan çok daha fazla olmaktadır.
2. Güvenlik duvarı, güvenlik politikalarının uygulanmasını sağlar. İnternet üzerinden sağlanan birçok hizmet güvenli değildir. Güvenlik duvarı, bir trafik polisi gibi görev yaparak, yalnızca güvenlik politikasına uyan hizmetlerin geçişine izin verir. Örneğin, NFS ve NIS/YP gibi internet üzerinden kullanımı riskli kabul edilen hizmetleri yerel ağ içerisinde tutar. Fakat bu hizmetlerin yerel ağ içerisinde kullanımı, güvenlik duvarı sisteminin kontrolü dışındadır.
3. Güvenlik duvarı, internet aktiviteleri konusunda verimli kayıtların (log) tutulmasını sağlar. İnternet ile yerel ağ arasındaki bütün trafik güvenlik duvarı üzerinden geçtiği için, sistemin ve ağın kullanımı hakkında bilgi toplamak ve gerekli kayıtları tutmak için en uygun noktadır.
4. Bazı durumlarda ağın bir bölümünün diğer bölümlerden daha iyi korunması gerekir. Bu durumda da güvenlik duvarı kullanılır. Amaç, bir bölümde oluşan sorunun diğer bölümlere sıçramasını engellemektir. Yine büyük bir yerel ağda bölümler arası trafiği kısıtlamak için de güvenlik duvarı kullanılabilir.

4.3.2. Güvenlik Duvarının Ağı Koruyamadığı Durumlar

Güvenlik duvarı, iyi bir ağ güvenliği sağlamasına rağmen, bazı tehlikeler güvenlik duvarı sisteminin kapsamı dışındadır. Bu tehlikelere karşı fiziksel önlemler alınmalı, bilgisayar (host) güvenliği sağlanmalı ve kullanıcılar eğitilmelidir.

1. Güvenlik duvarı, yerel ağ içerisindeki kötü niyetli kişilere karşı sistemi koruyamaz. Ağ üzerinden verinin çalınmasını engeller, fakat bazı kullanıcılar veriyi disk, kaset, disket ya da kağıt ortamında dışarı taşıyabilir. Yine kullanıcılar donanıma ve yazılıma zarar verebilir, programlar üzerinde ince değişiklikler yapabilir. Yerel güvenlik, bilgisayar (host) güvenlik önlemleri ve kullanıcıların eğitimi ile desteklenmelidir.

2. Güvenlik duvarı, kendi üzerinden gelmeyen bağlantılardan kaynaklanacak tehlikelere karşı sistemi koruyamaz. Örneğin, sisteme çevirmeli hatlar üzerinden erişime izin veriliyorsa, güvenlik duvarı bu yoldan gelecek tehlikelere karşı sistemi koruyamaz. Bazen uzman kullanıcılar ve sistem yöneticileri güvenlik duvarı sisteminin getirdiği kısıtlamalardan rahatsız oldukları için, sistemde kendileri için modem bağlantısı ile bir arka kapı oluştururlar. Güvenlik duvarı, bu hat üzerinden gelecek tehlikelere karşı sistemi koruyamaz, çünkü bu yönetimsel bir problemdir, teknik bir problem değildir.

3. Güvenlik duvarı, bilinen tehlikeleri önlemek üzere tasarlanır. İyi tasarlanmış bir güvenlik duvarı, yeni tehlikelere karşı da sistemi koruyabilir. Örneğin, güvenli olduğu hizmetlere izin verilir ve diğer bütün hizmetler engellenir. Birçok güvenlik duvarı sistemi, yerel ağı yeni tehlikelere karşı otomatik olarak koruyamaz. Saldırganlar zamanla sistemlere girmenin yeni yollarını bulmaktadırlar. Bu yüzden güvenlik duvarı sistemleri de zaman zaman güncellenerek, yeni güvenlik açıklarına karşı hazır hale getirilmelidir.

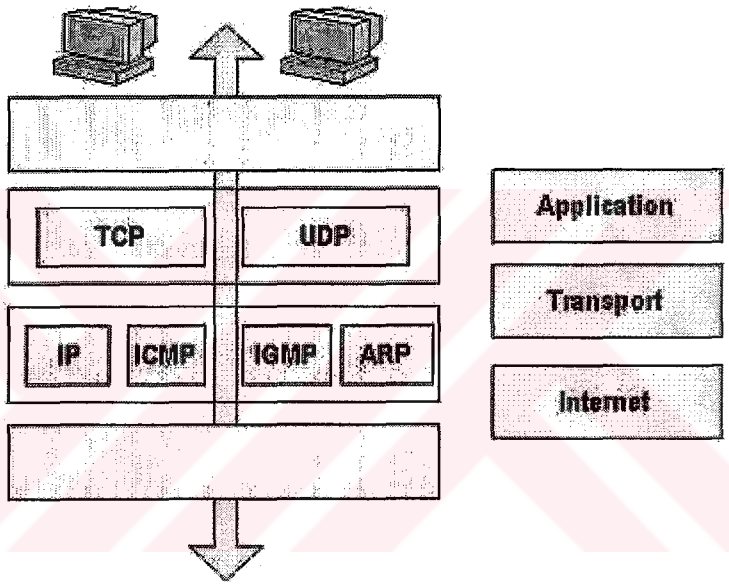
4. Güvenlik duvarı sistemleri, ağı virüslere karşı da koruyamaz. Bütün güvenlik duvarı sistemleri gelen paketleri tarar, bu tarama genellikle kaynak ve hedef adresleri, port ve protokol numaraları ile ilgilidir, verinin detayı ile ilgili değildir. Çok sayıda virüs türü vardır ve bunlar kendilerini birçok yolla veri içerisinde gizleyebilmektedir. Rastgele bir paket içerisinde virüs olduğunu anlamak çok zordur, çünkü paketin bir program parçası olduğunu, nasıl bir program gurubuna girdiğini ve programdaki değişimin virüsten kaynaklandığını belirlemek gerekir.

Bunlardan birincisi bile çok zordur. Çünkü bir güvenlik duvarı farklı formattaki programları çalıştıran bilgisayarları korumaktadır. Ayrıca, birçok program transfer sırasında sıkıştırılır ve paketlenir. Güvenlik duvarı virüsler konusunda çözüm sağlasa bile, virüs sisteme başka yollardan girebilir. Bu kullanıcılar aracılığıyla olabilir, paket programlar virüs içerebilir ya da çevirmeli hat ile internet üzerinden kopyalanan programlar virüs içerebilir. Virüslere karşı en iyi ve en pratik çözüm bilgisayar tabanlı, anti virüs programlarının kullanılması ve kullanıcıların virüs konusunda eğitilmesidir.

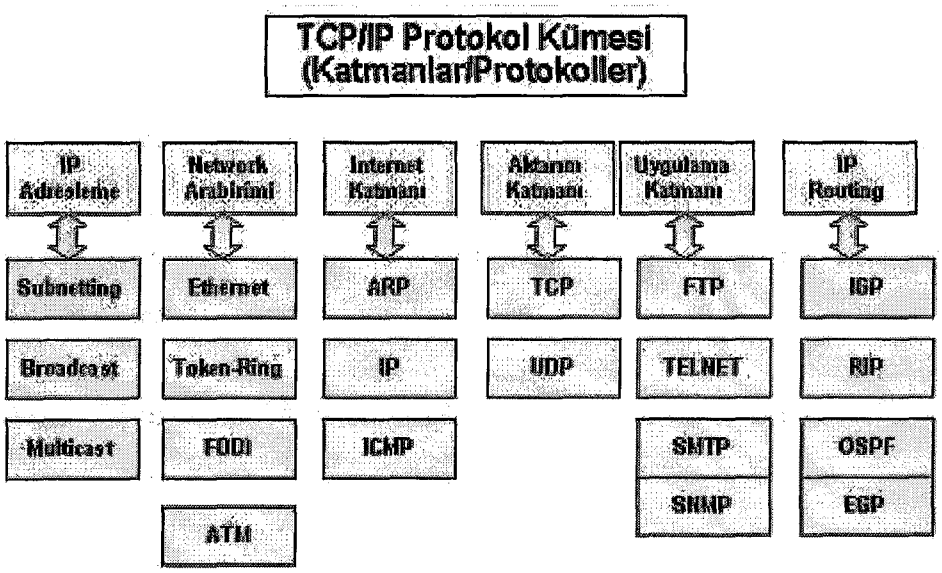
5. TCP/IP PROTOKOLÜ VE ŞİFRELEME

5.1. TCP/IP Protokolü

Başta Internet olmak üzere, farklı teknolojilere sahip ağların olması, bağımsız olarak yönetilmesi ve geliştirilmesi gibi özellikleri, TCP/IP protokolünün en yaygın kullanılan protokol olmasına neden olmuştur. Aslında, TCP/IP protokolü diye adlandırma yapmak çok doğru değildir. Çünkü TCP/IP çok sayıda protokol ve yardımcı programlardan oluşan bir protokol kümesidir (protocol stack) [4].



Şekil 5.1. TCP / IP Protokol Kümesi [4]



Şekil 5.2. TCP / IP Protokol Kümesi ve OSI Katmanları [4]

TCP/IP, endüstri standardı olan bir protokoldür. Bütün ağlar için geliştirilmiştir. TCP/IP, A.B.D. Savunma Bakanlığı projesi olarak, 1970' lerde temelleri atılmıştır. U.S. Department of Defense Advanced Research Projects Agency (DARPA) projesi, daha sonra ARPANET olarak kullanılmaya başlanmıştır. ARPANET adı verilen proje, üniversite ve kamu kuruluşlarını birbirine bağlamayı sağlayacak bir ağ geliştirme amacını taşımaktadır.

TCP/IP, DARPA' nın farklı bilgisayarlar arasında iletişim kurması gerektiğinde geliştirilmiştir. TCP/IP, işletim sistemi ve bilgisayardan bağımsız olarak bilgisayarların iletişim kurmasını planlamaktadır.

5.1.1. TCP/IP Mimarisi

TCP/IP protokol kümesi, altı çekirdek protokol ve bir dizi yardımcı program (utility) içerir. Altı çekirdek protokol:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- ARP (Address Resolution Protocol)

Tablo 5.1. TCP / IP Protokol Kümesindeki Yardımcı Programlar

Ping	Konfigürasyonu kontrol eder ve bağlantıyı test eder. Ping 131.140.1.1 şeklinde kullanılır.
FTP	Windows bilgisayarlar ile TCP/IP hostları arasında tek yönlü dosya transferini sağlar.
TFTP	Windows bilgisayarlar ile TCP/IP hostları arasında UDP kullanarak tek yönlü dosya transferini sağlar.
Telnet	Terminal öykünümünü sağlar.
RPC	UNIX host bilgisayar ile Windows bilgisayar arasında dosya kopyalar.
RSH	UNIX hostundaki komutları çalıştırır.
REXEC	Uzak bir bilgisayardaki bir işlemi çalıştırır.
Finger	Uzak bilgisayar hakkında bilgi sağlar.
ARP	Yerel olarak düzenlenmiş IP adreslerinin ön belleğini hazırlar.
IPCONFIG	Mevcut TCP/IP konfügürasyonunu gösterir.
NBTSTAT	IP adresleriyle düzenlenmiş NetBIOS bilgisayar adlarını görüntüler.
Netstat	TCP/IP protokolünün çalışması ilgili bilgileri görüntüler.
Route	Yerel yönlendirme tablosunu gösterir ve değiştirilmesini sağlar.
Hostname	RCP, RSH ve REXEC programlarının kimlik denetimini yaparak yerel bilgisayarın adını döndürür.

5.1.1.1. TCP (Transmission Control Protocol)

TCP protokolü, bağlantı tabanlı (connection-oriented) olarak adlandırılan, iki bilgisayar arasında veri transferi yapılmadan önce, bağlantının kurulmasını ve veri iletiminin garantili olarak yapılmasını esas alan bir protokoldür. TCP iletişiminde veri paketleri kullanılır. Ayrıca gönderen ve alan uygulamalarda da port bilgisi eklenir. Port (çıkış), kaynak ve hedef uygulamanın iletişimini sağlamaktadır.

TCP, güvenilir ve bağlantı (connection-oriented) temelli bir servistir. Bağlantı temelli olması, bağlantının bilgisayarlar arasında veri değişiminden önce yapılması anlamına gelmektedir. Güvenilir olması ise iletimin kontrolünün yapılması ile ilgilidir. Belli aralıklarla ACK bilgisi ile veri gönderimi kontrol edilmektedir.

TCP; byte-stream iletişimi kullanmaktadır. Bu yöntemde, TCP segmentlerindeki datalar bir bayt dizisi olarak işlenmektedir. Aşağıdaki tabloda TCP başlık bilgisi (header) içindeki ana alanlar yer almaktadır:

Tablo 5.2. TCP Başlık (Header) İçindeki Ana Alanlar

Alan	**İşlevi**
Source Port	Gönderen bilgisayarın TCP portu.
Destination Port	Alan (hedef) bilgisayarın TCP portu.
Sequence Number	TCP segmenti içindeki birinci baytın sıra numarası.
Window	TCP ara bellek (buffer) alanının şu anki mevcut büyüklüğü.
TCP Checksum	TCP header ve TCP datanın bütünlüğünü kontrol etmek için kullanılır.

5.1.1.2. UDP (User Datagram Protokol)

UDP, bir gönderim katmanı protokolüdür. Ancak, UDP iletiminde sağlama yapılmadığı için, gönderim garantisi olmamaktadır. Broadcast (genel yayın) iletiminde, az miktardaki verilerin iletiminde UDP paketleri kullanılmaktadır. UDP iletimi, gönderimin garanti edilmediği bağlantısız (connectionless) türü bir iletişim kurmaktadır.

5.1.1.3. IP (Internet Protocol)

Bu protokol, hedef bilgisayarın ağ (network) üzerindeki yerini bulmaktadır. Ayrıca, paketlerin adreslenmesini ve ağ üzerindeki bilgisayarlar arasında yönlendirilmesini sağlamaktadır. IP iletimi de UDP gibi gönderimin garanti edilmediği, bağlantısız (connectionless) türü bir iletişim kurmaktadır.

IP, iki bilgisayar (aygıt) arasında, paketlerin yönlendirilmesini sağlayan bağlantısız bir protokoldür. Bağlantısız (connectionless) olması, oturumun iletişimden önce kurulmamasıyla ilgilidir. Bununla birlikte, veri iletimindeki başarı da garanti edilmemektedir. İletimin garantisi, daha üst düzey protokol olan TCP ile sağlanmaktadır [5].

5.1.1.4. ARP (Adres Resolution Protocol)

Ağ üzerindeki bilgisayarların (host) birbirleriyle iletişim kurmaları için donanım adreslerini (MAC adresi) bilmeleri gerekmektedir. ARP, broadcast (genel yayın) temelli çalışan ağlarda, donanım adresini bulmak için kullanılmaktadır.

5.2. Şifreleme (Kriptografi)

5.2.1. Giriş

Şifreleme / deşifreleme (encryption-decryption); bir bilgisayar ağında veya kişisel bilgisayarlarda, haberleşme ya da dosya güvenliğini sağlamak için kullanılır. Bu nedenle, günümüzde bilgisayarlarda ya da bilgisayar ağlarında şifrelemenin önemi, gün geçtikçe artmaktadır.

İnternette yollanan veri paketleri, birçok halka açık ağlardan geçmekte, bu da bu paketlere ulaşmayı mümkün kılmaktadır. Son derece gizli bilgiler internette nakil olurken, bu durum önemli bir kaygı halini almaktadır. Bu tür bilgileri korumak mümkün olmadıkça, internette iş yapmak veya gizli şahsi yazışmalarda bulunmak asla güvenli bir yer olmayacaktır. Bilgi güvenliği başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin ortadan kaldırılması ile sağlanır ve bu amaçla kullanılan temel araç, kriptografidir. Kriptografi, bilgi güvenliğini inceleyen ve anlaşılabileni anlaşılamaz yapan bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine yapılan çalışmalar, kriptografinin önemli konularıdır.

Kriptografi genel olarak şu ana konularla ilgilenir:

Gizlilik: Bilgi istenmeyen kişiler tarafından anlaşılamamalıdır.
Bütünlük: Bir iletinin alıcısı, bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememelidir.
Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememelidir. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu, yanlışlıkla reddetmemelidir.
Kimlik belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir, başkasının kimliğine bürünme şansına erişmemelidir.

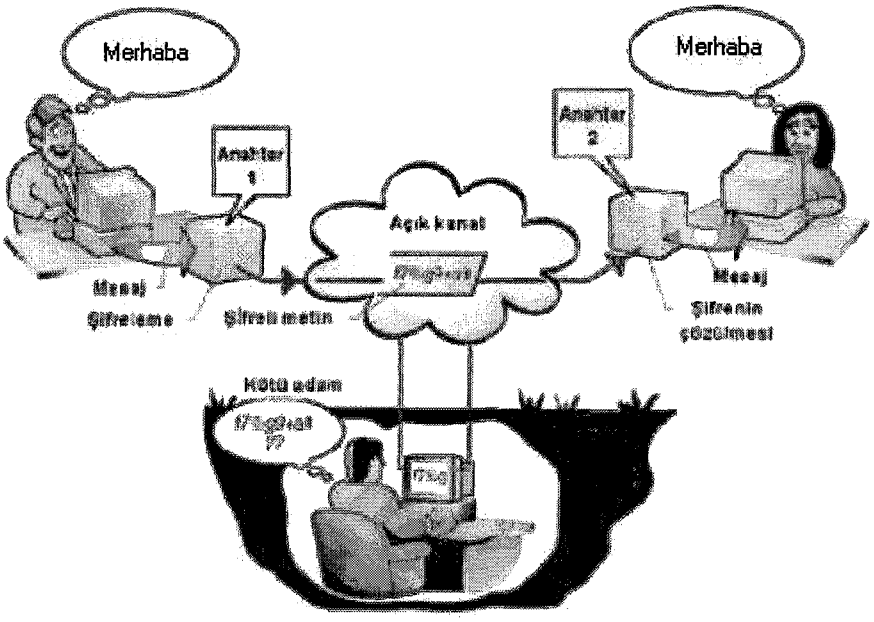
5.2.2. Şifrelemenin Temel Elemanları

Bir gönderici, bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler, üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar. Burada söz konusu ileti, düz metindir. Bazı kullanımlarda *plaintext* adı da verilir.

Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (*encryption*). Bu işlem, düz metini şifreli metine dönüştürür. Böylelikle bilgi içeriği, başkalarının anlamayacağı hale gelmektedir. Bu bilgi, bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir bilgi olabilmektedir. Şifrelenmiş bir ileti, şifreli metindir (*ciphertext*). Şifreli metini düzmetine geri çevirme işlemi, şifre çözümüdür (*decrypt*).
Bu işlemler **Şekil 5.3.**'de gösterilmektedir.

Şekil 5.3. Şifreleme ve Şifreyi Çözme İşlemleri [6]

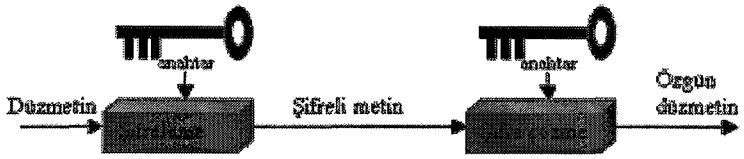
İleti güvenliğini sağlama bilimi, kriptografidir. Matematiğin hem şifrebilimi hem de şifre analizini kapsayan dalı kriptolojidir ve şifrebilimciler tarafından icra edilmektedir. Eğer bir algoritmanın güvenliği, bu algoritmanın çalışma biçimini gizlemeye dayalıysa, bu bir sınırlandırılmış algoritmadır. Sınırlandırılmış algoritmalar günümüzün şartlarına pek uymamaktadır. Bir gruba ait kullanıcılar bunları kullanamamaktadır, çünkü gruptan bir kullanıcının her çıkışında, geri kalan herkesin başka bir algoritmaya geçmesi gerekmektedir. İçlerinden birisi yanlışlıkla gizleneni açığa vurduğunda, diğer herkesin algoritmalarını değiştirmeleri gerekmektedir. Daha da kötüsü, sınırlandırılmış algoritmalar, kalite kontrolüne ve standartizasyona olanak tanımamaktadır. Her bir grup kullanıcının kendisine ait bir algoritması olmalıdır. Bu tür bir grup, hazır şifre çözüm anahtarının yazılım veya donanım ürünlerini kullanamaz; davetsiz bir misafir aynı ürünü alıp algoritmayı öğrenebilir. Kendi algoritmalarını ve gerçekleştirimlerini kendileri yazmaları gerekir. Günümüz kriptografisi, bu sorunu bir anahtar ile çözmektedir. Bu anahtar, çok çeşitli değerler alabilen herhangi bir anahtar olabilir. Günümüzde kullanılmakta olan modern ve güçlü şifreleme algoritmaları, artık gizli değildir. Bu algoritmalar güvenliklerini, kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlarlar. Bütün modern algoritmalar şifrelemeyi ve şifre çözmeyi kontrol için anahtarları kullanmaktadır. Bir anahtar ile şifrelenmiş bilgi, kullanılan algoritmaya bağlı olarak, ilgili anahtar ile çözülebilir. Genel olarak anahtarın kullanımı aşağıdaki şekildedir (**Şekil 5.4.**) :



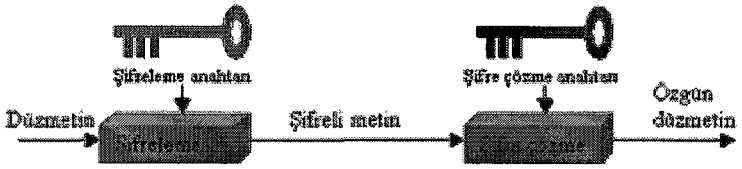
Şekil 5.4. Bir Mesajın Dinlenmesini Önlemek için Anahtar ile Şifreleme [6]

Kullanıcı bir mesajı (m) göndermeden önce bir anahtar (k1) kullanarak şifreler. Şifreli metin (c), yasadışı dinleyicilere açık olan bir kanaldan gönderilir. Mesajı okumak için alıcı, bir anahtar (k2) kullanarak şifreyi çözer ve m mesajını elde eder. Aktif düşmanlar araya girip iletişimi dinleyebilir. Eğer k1 ve k2 eşitse, sistem simetriktir. Aksi takdirde bu sistem, asimetrik olarak nitelendirilmektedir. Güvenliğin garantilenmesi için k2, her zaman gizli olmalıdır, ancak k1' i kullanarak, k2' yi elde etmek mümkün olmadığı sürece, k1 açıklanabilir. Bu durumda sisteme açık anahtarlı sistem (public key system) adı verilmektedir.

Açık anahtarlı sistemler pek çok ilginç olanaklar sunar; örneğin herkes online bir mağazaya, mağazanın açık k1 anahtarını kullanarak, şifrelenmiş bir kredi kartı numarası gönderebilir. k2 anahtarını sadece mağaza bildiği için, kartın numarasını sadece mağaza öğrenebilir. Eğer simetrik sistem kullanılsaydı, mağaza potansiyel müşterilerinin her biriyle önceden ve gizlice ayrı ayrı anahtarlar belirlemek zorunda kalırdı. Açık anahtarlı sistemlerin güvenliği, her zaman belirli matematiksel problemleri çözmenin zorluğuna dayanır, simetrik sistemler daha çok tek kullanımlık, geçici yapıdadırlar. Açık anahtarlı sistemlerin en büyük dezavantajı, matematiksel yapıları nedeniyle simetrik sistemlerden daha yavaş olmalarıdır; özellikle açık anahtarlı sistemlerdeki anahtarların boyutları, simetrik sistemlerin anahtarlarının boyutlarından çok daha büyüktür. Kısaca, kullanılacak şifreleme yöntemi gerçekleştirilecek uygulamaya bağlı olarak seçilir (**Şekil 5.5.**).



Şekil 5.5-a Tek Anahtar ile Şifreleme



Şekil 5.5-b İki Farklı Anahtar ile Şifreleme

Algoritmalardaki bütün güvenlik, anahtara (veya anahtarlara) dayalıdır, hiçbiri algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenebildiği anlamına gelir. Bu algoritmayı kullanan ürünler seri üretilebilir. Bir davetsiz misafirin sizin algoritmanızı bilmesi önemli değildir; sizin özel anahtarınızı bilmedikçe, o şahıs iletilerinizi okuyamaz.

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki kategoriye ayrılmaktadır. Bu yöntemler:

- Gizli-Anahtar (Simetrik) yöntemleri (Geleneksel kriptolama sistemleri)
- Açık-Anahtar (Asimetrik) yöntemleri (Açık anahtar kriptolama sistemleri)

5.2. 3. Açık Anahtarlı Şifreleme

Açık anahtarlı kriptografinin gelişmesi, bütün kriptografi tarihindeki en büyük devrimdir. Başlangıcından günümüze kadar bütün kriptografik sistemler, süpstütüsyon ve permütasyon işlemlerinin temel alınmasıyla oluşturulmuştur. Sadece elle hesaplanabilen algoritmalarla çalışabilme döneminden sonra, şifreleme / deşifreleme yapan rotor makinelerinin ortaya çıkması sonucunda, geleneksel kriptografide büyük bir gelişme kaydedilmiştir. Elektromekanik rotor, çok fazla inceliklere sahip ve karmaşık kriptografik sistemlerin geliştirilebilmesini sağlamıştır. Mevcut bilgisayarlarla, daha karmaşık sistemler tasarlanmış ve en tanınanlarından olan IBM′ in Lucifer girişimi gelişerek DES şifrelemeyi oluşturmuş ve DES` i dünyadaki kriptografi teknikleri arasında en yüksek seviyeye getirmiştir. Rotor makineleri ve DES (Data Encryption Standart), önemli avantajlar sunmalarına rağmen, halen süpstütüsyon ve permütasyon işlemlerine bağımlı kalmaktadır.

Açık anahtarlı kriptografi, daha önceki gelişmelerden radikal bir kopuş olmuştur. Açık anahtarlı kriptografik sistemlerin en önemli noktaları, süpstütüsyon ve permütasyondan çok, matematiksel işlevler üzerine temellenmiş olmalarıdır. Daha da önemlisi, açık anahtarlı kriptografi, tek anahtar kullanan simetrik (geleneksel şifreleme) algoritmaların tersine, iki ayrı anahtarın asimetrik kullanımını öngörmektedir. Anahtar dağıtımı ve kimlik denetimi gibi gizlilik ve güven gerektiren durumlarda, iki anahtar kullanımı etkili sonuçlar ortaya koymaktadır.

Açık anahtarlı şifreleme ile ilgili bazı yaygın, yanlış bilgiler söz konusu olmaktadır. Bu yanlış düşüncelerden birisi, açık anahtarlı şifrelemenin, kriptoanalize karşı geleneksel şifreleme yöntemlerinden daha güvenli olduğudur. Örneğin böyle bir iddia, Gardner' ın meşhur *Scientific America* adlı 1977 yılında yayınladığı makalesinde yapılmıştır. Aslında, şifrelemenin güvenliği, anahtarın uzunluğuna ve kırılan şifreli metnin içerdiği hesapsal işlemlerin karmaşıklığına dayanmaktadır. İster geleneksel, ister açık anahtarlı şifreleme olsun, kriptonaliz bakış açısına göre birini direğinden üstün tutmak yanlış olmaktadır. Bir ikinci yanlış düşünce de genel amaçlı kullanım için geliştirilmiş bir teknik olan açık anahtarlı şifrelemenin, geleneksel şifrelemeyi modası geçmiş kıldığıdır. Tam tersine, geleneksel şifrelemeden vazgeçileceği sanısı, açık anahtarlı şifreleme yöntemlerinin matematiksel fonksiyonlarından dolayı, ihtimal dışı gözükmektedir [6].

Son olarak, açık anahtarlı şifreleme kullanılırken, geleneksel şifrelemenin daha hantal anahtar dağıtım merkezleri ile karşılaştırıldığında, açık anahtarlı sistemlerin anahtar dağıtımının üzerinde kafa yorulması gerekmeyen, sıradan ve basit bir iş olduğuna dair yanlış bir anlayış vardır. Aslında, protokolün bazı biçimleri gereklidir, fakat geleneksel şifreleme yöntemlerinin ihtiyaç duyduğu merkez temsilciler ve prosedürler, açık anahtarlı şifrelemenin ihtiyaç duyduklarından daha basit, daha karmaşık ya da daha etkili değildir.

Açık anahtarlı kripto sistemlerinin çoğunluğu, sayılar teorisini temel almaktadır. Açık anahtarlı şifreleme algoritmaları hakkında kesin bir yargıya varmak için, sayılar teorisinin bazı kısımlarını bilmek gerekmektedir.

Tablo 5.3, geleneksel ve açık anahtarlı şifrelemenin farklarını açıkça göstermektedir. Geleneksel şifrelemede kullanılan anahtarı, açık anahtarlı şifrelemede kullanılan anahtarlardan ayırmak için, bu anahtara **gizli anahtar** adı verilmektedir. Açık anahtarlı şifrelemede kullanılan iki anahtar da **genel anahtar** ve **özel anahtar** olarak isimlendirilmektedir.

Özel anahtar, her zaman gizli tutulacak olan anahtardır, fakat geleneksel şifrelemedeki gizli anahtarla karışmaması için, ona gizli anahtar yerine özel anahtar denilmesi daha doğru olmaktadır.

Tablo 5.3. Geleneksel ve Açık Anahtarlı Şifreleme [6]

Geleneksel şifrelemede:	Açık anahtarlı şifrelemede:
Çalışması için:	
1.Şifreleme ve Deşifreleme için aynı algoritma aynı anahtarla birlikte kullanılır.	1. Şifreleme ve Deşifreleme için bir algoritma ve anahtarlardan birisi kullanılır. Şifreleme için kullanılan anahtar, de-şifreleme için kullanılamaz.
2. Gönderen ve alan, algoritmayı ve anahtarı paylaşmalıdır.	2. Gönderen ve alan, ilişkili anahtarlardan birine sahip olmalıdırlar (aynı olanı değil).
Güvenlik için:	
1. Anahtar gizli tutulmalıdır.	1. Anahtarlardan biri gizli tutulmalıdır.
2. Diğer bilgiler saklandığında, mesajı deşifre etmek imkansız olmalıdır.	2. Diğer bilgiler saklandığında, mesajı deşifre etmek imkansız olmalıdır.
3. Algoritma ve şifreli metin örnekleri bilmek, anahtarı çözmek için yetersiz olmalıdır.	3.Algoritma ve şifreli metin örnekleri bilmek veya anahtarlardan birine sahip olmak, diğer anahtarı bulmak için yetersiz olmalıdır.

5.2.3.1. Açık Anahtarlı Kripto Sistem Uygulamaları

Açık anahtarlı sistemler, karakteristik olarak birisi gizli tutulan, diğeri ise genel kullanım için açılmış olan iki anahtarla çalışan kriptografik algoritmalar kullanmaktadır. Uygulamaya bağımlı olarak, gönderici ya kendisinin özel anahtarını, ya alıcının genel anahtarını ya da ikisini birden, kimi kriptografik fonksiyonları gerçeklemek için kullanmaktadır. Geniş bir bakış açısı ile açık anahtarlı kripto sistemlerin kullanımı, üç kategoride incelenebilir:

- **Şifreleme / Deşifreleme:** Gönderici, bir mesajı alıcının genel anahtarı ile şifreler.
- **Dijital İmza:** Gönderen, mesajı kendi özel anahtarı ile imzalar. Bu imzalama, mesajın tamamını ya da önemli görülen belirleyici bir kısmını şifrelemek ile yapılır.
- **Anahtar Değişimi:** İki taraf ortaklaşa bir oturum anahtarını değiş tokuş ederler. Birçok farklı yöntem mümkündür.

Kimi algoritmalar, bu özelliklerden sadece bir ya da iki tanesini gerçekleştirebilirken, bazıları bunların tümünü gerçekleştirebilir. **Tablo 5.4.** , kimi açık anahtarlı algoritmaların bu özelliklerden hangilerini desteklediğini göstermektedir.

Tablo 5.4. Açık Anahtarlı Kripto Sistemler için Uygulamalar

Algoritma	Şifreleme / Deşifreleme	Dijital İmza	Anahtar Değişimi
RSA	Evet	Evet	Evet
Diffie-Hellman	Hayır	Hayır	Evet
DSS	Hayır	Evet	Hayır

6. GÜVENLİK DUVARI UYGULAMASI-I

6.1. Giriş

Tezin uygulama bölümü için ilk olarak ISA sunucu sistemi oluşturulmuştur. Tez uygulamasında kullanılan yazılım ve donanımlar aşağıda verilmiştir:

- Çarpraz (Crossover) kablo
- 2 adet Bilgisayar
- 2 adet Ethernet kartı
  - ✓ D-LİNK DFE 538 TX 10/100 Adapter (İç ağ için)
  - ✓ INTEL® PRO/100 ve Network Connection (Dış ağ için)
- Windows 2000 Advanced server programı
- ISA Server 2000 programı

6.2. Windows 2000 Advanced Server

Microsoft® Windows® 2000 Advanced Server işletim sistemi, standart Windows 2000 server sürümünün özelliklerine ve işlevlerine sahip olmanın yanı sıra, yüksek düzeyde ölçeklenebilirlik, güvenirlik ve sürekli çalışırlık gerektiren büyük organizasyonlara yönelik ek özellikler sunmaktadır.

Windows 2000 Advanced Server, gelişmiş simetrik çok işlemcili teknolojisi ile entegre sistem ölçeklenebilirliği sağlamasına ek olarak iki ilave teknoloji (kümeleme, TCP/IP yük dengeleme) sayesinde kullanım düzeyi ve çoklu sistem ölçeklenebilirliğini en üst düzeye çıkarmaktadır [7].

Pahalı olmayan kişisel bilgisayar donanımıyla çalışabilen Windows 2000 Advanced Server, pahalı olan ve yüksek kullanım düzeyi sunan çözümlere karşı organizasyonlara güçlü ve ölçeklenebilir bir alternatif sunmaktadır. Windows 2000 Advanced Server; e-ticaret, kurumsal Internet ve Intranet siteleri, veritabanları ve kurumsal kaynak planlama (ERP) uygulamaları gibi uygulama ve hizmetler için idealdir. Aşağıda Windows 2000 Advanced Server' a ait özellikler verilmiştir:

- Gelişmiş Simetrik Çok İşlemcili (SMP) Ölçeklenebilirlik
- Yüksek Kullanım Düzeyi Sunan Kümeleme
- Sürüm Yükseltme Desteği
- Ağ Hatalarından Kurtulma
- Durum İzleme
- Ağlar ve Disketler için Tak ve Çalıştır hizmeti
- WINS, DFS ve DHCP desteği
- Küme API için COM Desteği
- TCP/IP Ağ Yük Dengeleme (NLB)
- Yüksek Kullanım Düzeyi
- Denetim Kolaylığı
- Kullanım Kolaylığı
- Kurumsal Bellek yapısı

6.3. ISA Server 2000

Microsoft Internet Security and Acceleration (ISA) Server 2000, politika tabanlı güvenlik uygulamaları sunan, ağ yapılarını hızlandıran ve bu yapıların etkin biçimde yönetilmesini sağlayan bir güvenlik duvarı (firewall) ve Web önbellek (cache) sunucusudur. Firewall bileşeni; paket seviyesinde anahtarlama ve uygulama seviyelerinde filtreleme yapma, üzerinden geçen veri trafiğini kapsamlı biçimde inceleme ve trafiğin erişim politikalarını ve yönlendirilmesini kontrol etme özelliğine sahiptir. Önbellek bileşeni ise, sıkça kullanılan Web içeriğini önbellekte depolayarak ağ performansının ve kullanıcı deneyiminin artmasını sağlamaktadır. Güvenlik duvarı bileşeni ve önbellek bileşeni, farklı sunuculara kurulabileceği gibi, tek bir makine üzerinde de bulunabilmektedir [7].

ISA Server kullanıcılara Standart sürüm (edition) ve Enterprise Edition olarak iki farklı versiyonla sunulmaktadır. Her iki versiyon da zengin özellikler içermektedir. Standart Edition, en fazla dört işlemciyi destekleyen tek bir sunucu için tasarlanmıştır. Daha geniş uygulama alanları için tasarlanan Enterprise Edition, sunucu grupları oluşturmak, çok katmanlı politikalar geliştirmek ve dört işlemciden daha fazla işlemciye sahip sistemler için uygundur. ISA Server ' ın sunduğu özellikler farklı kategorilerde ele alınabilir. Bunlar:

- **Güvenli İnternet Bağlantısı**

Günümüzde yerel ağların İnternet'e bağlanması, güvenlik ve verimlilik açısından birçok sorunun yaşanmasını da beraberinde getirmektedir. Bu sıkıntıların aşılması için işletmeler

önemli ölçüde teknolojik altyapı oluşturmak zorundadır. ISA Server, kullanımın izlenmesine ve erişimin kontrol edilmesine yönelik sağladığı araçlar ile birçok süreci otomatize ederek sistem yöneticilerinin, işle ilgili sorunların çözülmesine daha fazla zaman ayırmalarına imkan tanımaktadır. ISA Server, ağları yetkisiz kullanıcıların erişiminden korur, trafiği denetler ve saldırıları sistem yöneticilerine bildirir.

ISA Server; çok katmanlı kurumsal güvenlik duvarı, durumsal denetim, sanal özel ağ çözümü (VPN), geniş uygulama desteği, entegre izinsiz saldırı (intrusion detection), akıllı uygulama filtreleri ve gelişmiş doğrulama gibi birçok özelliğe sahiptir.

- **Çok Katmanlı Güvenlik Duvarı**

Bir güvenlik duvarı, kullandığı çeşitli yöntemler aracılığıyla güvenlik özelliklerinin zenginleştirilmesini sağlar. Bu yöntemlerden başlıcaları; paket filtreleme, anahtarlama seviyesinde filtreleme ve uygulama filtrelemedir. ISA Server gibi gelişmiş güvenlik duvarı (firewall) çözümleri, birden fazla ağ katmanına yönelik bu yöntemleri birleştirerek çok katmanlı bir yapı ortaya koymaktadır. Paket filtreleme, ISA Server üzerinden geçen IP paketlerinin akışının kontrolüne imkan vermektedir. Paket filtreleme kullanıldığında paketlerin geçişi; statik olarak IP filtreleri veya dinamik olarak erişim politikası ve yayınlama kurallarının izin verdiği biçimde sağlanır.

Dinamik paket filtrelemede, bir iletişim gereksinimi olduğu anda portlar otomatik olarak açılır ve bu iletişim sona erdiğinde otomatik olarak kapanmaktadır. Bu sayede savunmasız kalan portların sayısı minimize edilerek, daha yüksek seviyede bir güvenlik sağlanmaktadır. Anahtarlama seviyesinde filtreleme; Telnet, posta, Microsoft Windows Media, RealAudio, IRC gibi birçok İnternet uygulaması ile birlikte çalışmaktadır. Bu filtre ile sözü geçen programların, herhangi bir sorun yaşamadan internetle bağlantı kurmalarına izin verilmektedir. Ayrıca bu filtre yardımı ile oturumların izlenmesi de mümkün olmaktadır. Uygulama filtreleri, bir firewall çözümünün en karmaşık noktası olan uygulama seviyesinde trafik izleme özelliğinin gerçekleşmesini sağlar. Bu filtreler, belirli uygulamalardan gelen verileri analiz eder ve her uygulamaya özel izleme, engelleme, yönlendirme veya değiştirme işlemleri gerçekleştirmektedir.

ISA Server' ın en önemli özelliklerinden birisi de, ICSA laboratuarları tarafından sertifikalandırılmış olmasıdır. ICSA laboratuarları, güvenlik ürünleri konusunda çeşitli testler ve değerlendirmeler gerçekleştiren bağımsız ve güvenilir bir kuruluştur. Bu süreç, ürünün ICSA' nın test ortamına yüklenmesi ile başlayan ve çeşitli tarama yöntemleri kullanılarak gerçekleştiren bir dizi testten oluşmaktadır. ISA Server, normalde 90-120 gün süren bu test sürecini, 30 gün gibi kısa bir sürede geçerek, birçok yeni ürünün başarısız olduğu bu önemli

testte, ciddi bir başarı elde etmiştir. Güvenlik teknolojileri sektöründe oldukça saygı gören bu sertifika, ISA Server' ın öncü ve etkin yapısının en güzel kanıtlarından birisidir.

- **Durumsal Denetim**

ISA Server, ağ servisini veya kullanılan uygulamayı paket seviyesinde tanımlayarak, IP protokolünün başlığında belirtilen trafiğin başlangıç noktasını ve TCP protokolündeki portu izlemektedir. Bu özellik sayesinde, korumasız kalan portların sayısının minimize edilmesi ve ağ içesinde çok daha yüksek seviyede bir güvenliğin oluşturulması mümkün olmaktadır.

- **Geniş Uygulama Desteği**

ISA Server, yapısal olarak 100' den fazla protokolü tanımlar ve yöneticiye port numarasına, tipine, TCP veya UDP özelliklerine göre ilave protokoller tanımlama imkanı sunmaktadır. Bunun yanında ISA Server, herhangi bir özel istemci yazılımına sahip olmayan, herhangi bir işletim sistemi veya platform üzerinde çalışan istemci bilgisayarlar için, SecureNAT kullanarak, şeffaf ve yaygın bir destek sağlamaktadır.

- **Entegre Sanal Özel Ağ**

Sanal özel ağ (VPN), özel bir ağın, İnternet gibi genel ve paylaşılan bir ağa olan uzantılarıdır. Bir Sanal Özel Ağ (VPN) yardımı ile paylaşılan bir genel ağ üzerinden iki bilgisayar arasında sanki uçtan uca özel bir ağ kurulmuşçasına bilgi iletmek mümkün olmaktadır. ISA Server, İnternet üzerinden güvenli bir bilgi alışverişinin gerçekleştirilmesi için, bir VPN gibi konfigüre edilebilmektedir.

- **Sistem Kararlılığı**

ISA Server, temelinde bulunan Windows 2000 Server işletim sisteminin güvenli kılmasına yönelik bir sistem güvenlik sihirbazını da içermektedir. Bu araç yardımı ile bir sistem yöneticisi çeşitli seçenekler yardımı ile farklı güvenlik seviyeleri belirleyebilecektir.

- **Entegre İzinsiz Saldırı (Intrusion Detection)**

ISA Server, bir izinsiz saldırı (intrusion detection) mekanizması olarak da kullanılabilir. Bu mekanizma, ağa bir saldırı olduğu durumda devreye girmektedir. Güvenlik duvarı (firewall) yöneticisi, belirli bir saldırı olduğu takdirde, kendisini uyaracak çeşitli alarmlar tanımlama şansına sahiptir. Bunun yanında bir saldırı söz konusu olduğunda, sistemin ne şekilde davranacağı da belirlenebilmektedir.

- **Akıllı Uygulama Filtreleri**

Uygulama filtreleri, güvenlik duvarı (firewall) servisinin birer uzantısıdır. Bu filtreler, verinin izlenmesi ve işlenmesiyle birlikte trafiğin, protokollere özel bir biçimde analizi ve yönetilmesini gerçekleştirmektedir. Uygulama filtreleri, bir firewall servisi oturumu içerisinde gerçekleşen veri akışına veya datagramlara erişmektedir. Bunun yanında uygulama filtreleri, doğrulama veya virüs taraması gibi sisteme özel görevleri yerine getirebilmektedir.

- **Gelişmiş Doğrulama Özellikleri**

ISA Server, erişim politikalarını ve yayınlama kurallarının, belirli terminal gruplarının veya kullanıcı gruplarının belirlenen sunuculara erişimini engelleyecek ya da mümkün kılacak şekilde yapılandırılmasına imkan vermektedir. Gelen ve giden Web taleplerinin ayarları, kullanıcıların, kuralları uygulamadan önce her seferinde tekrardan doğrulanmasına yönelik olarak yapılabilmektedir. Bunun yanı sıra hangi doğrulama yönteminin kullanılacağının belirlenmesi ve farkı doğrulama yöntemlerinin kullanılabilmesi de mümkündür.

- **Güvenli Yayınlama**

ISA Server, çeşitli servislerin, güvenlikten herhangi bir taviz vermeden kolaylıkla İnternet ortamında yayınlanmasını sağlamaktadır. Bunun gerçekleştirilmesi için, Web yayınlama sunucusu ve bir sunucu üzerindeki yayınlama kuralları, dahili sunucular üzerinde artırılmış bir güvenlik sağlayacak şekilde yapılandırılabilmektedir.

- **Elektronik Posta İçerik İzleme**

Posta sunucularına yetkisi olmayan kullanıcılar girişinin engellenmesi ve kabul edilmeyen elektronik postaların, geçit bölgelerinde durdurulmasına yönelik özelliktir.

- **SSL trafiğinin izlenmesi**

Secure Socket Layer (SSL) köprüleme yöntemi kullanılarak uçtan uca bir güvenlik sağlanıp, şifrelenmiş SSL trafiğinin izlenmesine müsaade etmektedir.

6.4. ISA Server 2000' in Kurulum Aşamaları

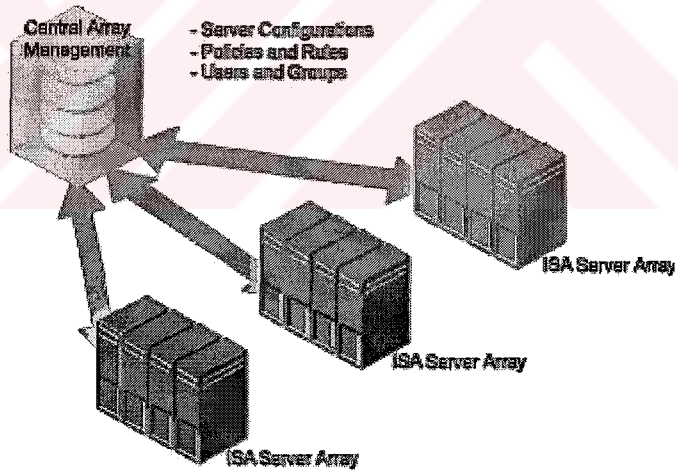
ISA Server 2000 programının iki farklı sürümü bulunmaktadır:

a) Standart Sürüm

Daha çok küçük ölçekli ağlarda ve iş istasyonlarında tercih edilmektedir. Maksimum 4 işlemci desteklemektedir. Sistemde oluşturulan kurallar sunucu üzerinde saklanmaktadır. Bunun anlamı, Aktif Dizin (Active Directory) ile tümleşik olarak hareket edemeyeceğidir.

b) Enterprise Sürüm

Standart sürümden farkı, aktif dizin (active directory) ile tümleşik olarak çalışmasıdır. Bu sayede, oluşturulan kurallar aktif dizin içerisinde saklanır. Böylece bir dizi (array) oluşturup, sistemde bir ISA Server üzerinde oluşturulacak kuralların, diğerlerine yansımasını sağlamak mümkün olmaktadır. Sonuçta, merkezi bir yönetim sağlanmış olduğu gibi, yükün balanslanması (load balancing), hata toleransı (fault tolerance) ve dağıtık önbellek (distributed caching) özelliklerinden de faydalanılabilmektedir. Bu versiyonun herhangi bir donanım kısıtlaması yoktur **(Şekil 6.1.).**



Şekil 6.1. ISA Sunucu Yapısı [7]

6.4.1. ISA Server 2000 Donanım Gereksinimleri

Microsoft firmasının, bu sunucu kurulumu için tavsiye ettiği minimum donanım gereksinimleri şunlardır:

CPU : 300 Mhz veya üstü Pentium II işlemci
RAM : 256 MB
HDD : 20 MB ve NTFS Partition
OS : Windows 2000 (Minimum Service Pack 1) veya Windows 2003 Server Ailesi
NIC : Windows 2000 uyumlu Ethernet

Ayrıca Array konfügürasyonu için, aktif dizin zorunludur. Ethernet kartı olarak kartlardan bir tanesi iç ağ, diğer kart ise ADSL vb. cihazın bağlı olacağı dış ağ'a bakan karttır. Dış ağ'a bakan kart üzerinde, Netbios over TCP özelliğini pasif yapmak faydalı olacaktır. İç ağ'a bakan kartın ağ (network) özelliklerinde herhangi bir default geçityolu (gateway) girilmemesi gereklidir, aksi halde yerel ağ (network) üzerindeki internet çıkışında, sorunlar meydana gelebilmektedir [8].

6.4.2. ISA Server Kurulum Modları

a) Cache Mode

Adından da anlaşılacağı üzere, bu mod ile kurulum yapıldığında ISA Server, sadece Cache olarak çalışmakta, güvenlik duvarı olarak herhangi bir fonksiyonu bulunmamaktadır. Normalde yerel bir bilgisayarda bir internet sayfası ziyaret edildiğinde, bu sayfa o bilgisayarın kendi ön belleği (cache)' inde depolanır ve bir sonraki sefere daha hızlı olarak sayfaya erişilebilmektedir. ISA Server sayesinde gezilen sayfalar, hatta ftp ve http üzerinden yüklenen (download) edilen dosyalar bile ön belleğe alınabilmekte ve bu ön bellek (cache) tüm ağ için geçerli olmaktadır. Neticede gözle görülür bir performans artışı olmakla beraber, gereksiz yere band genişliği de kullanılmayacaktır. Sunucu üzerinde büyük kapasiteli ve SCSI bir disk olması performans olarak büyük fayda sağlayacaktır.

b) Firewall Mode

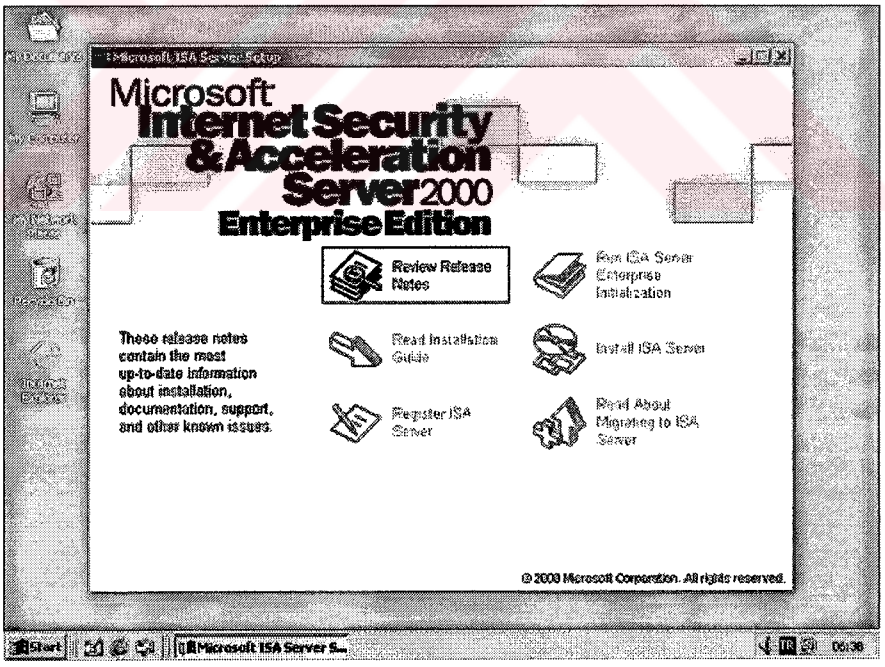
Güvenlik duvarı (Firewall) olarak kurulum yapılan bu modda, kurulumdan sonra internet ile yerel ağ arasında bulunan tüm portlar kapatılmaktadır. Ağ yapısına ve güvenlik politikasına uygun olarak oluşturulacak kurallar sayesinde, gerekli portlar açılmalı ve böylece maksimum güvenlik sağlanmalıdır.

c) Integrated Mode

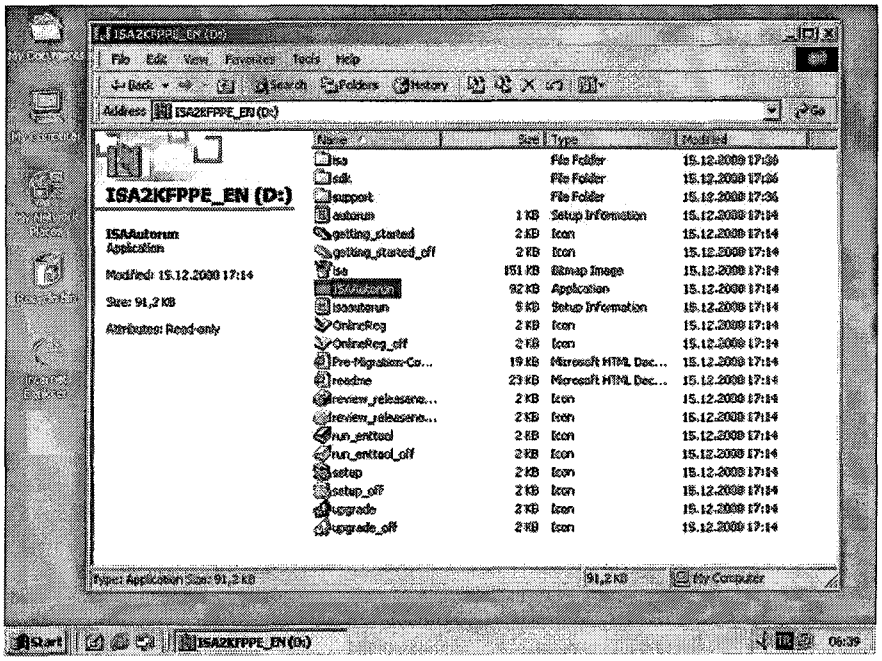
Bu mod ile kurulum yapıldığında, Cache ve Firewall birlikte çalışacaklardır. Tavsiye edilen moddur.

6.4.3. ISA Server Enterprise Sürüm Kurulum Aşamaları

ISA Server 2000 Cd' si Cd-Rom sürücüye takılır. Eğer Otomotik başlat (Auto Start) özelliği pasif değil ise setup ekranı otomatik olarak açılacaktır **(Şekil 6.2.).** Eğer setup ekranı otomatik olarak gelmez ise Cd içerisinden **"ISAAutorun"** öğesine çift tıklanmak suretiyle, setup ekranının açılması sağlanmış olur **(Şekil 6.3.).**

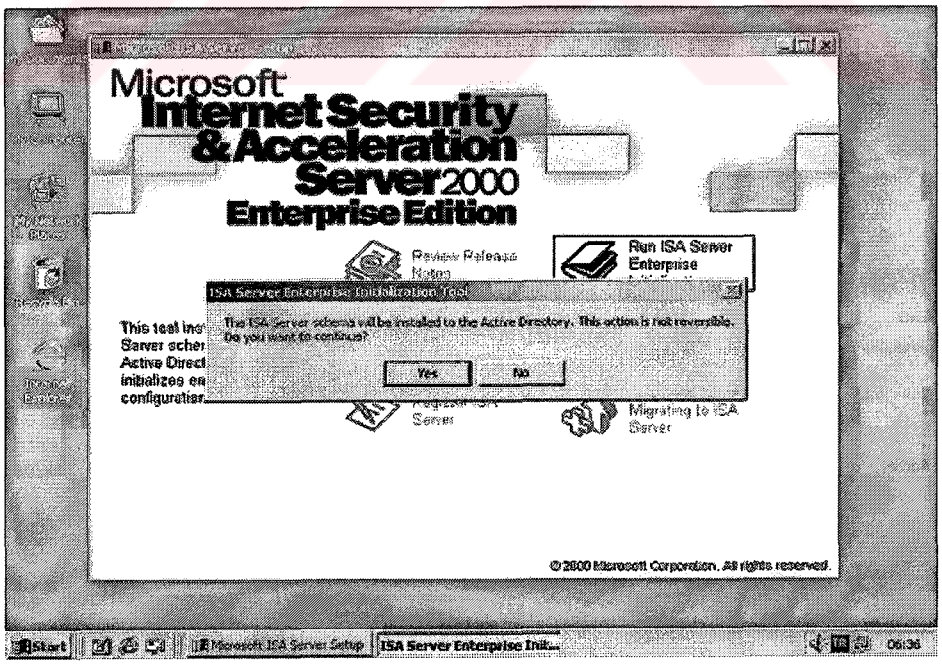


Şekil 6.2. Setup Ekranı



Şekil 6.3. ISAAutorun Öğesinin Görünümü

ISA Server'ın Active Directory ile tümleşik çalışması isteniyorsa, kurulumdan önce önemli bir işlem yapılması gerekmektedir. **Şekil 6.2'** de görülen setup ekranındaki **"Run ISA Server Enterprise Initialization"** tıklanmalıdır. Daha sonra **Şekil 6.4'** de görülen uyarı ekranı çıkacaktır, burada **"yes"** seçilmelidir.



Şekil 6.4. Aktive Dizin için Uyarı Ekranı

Şimdi karşımıza, **Şekil 6.5'** de görülen ekran gelmiş olmalıdır. Bu ayarları kurulumdan sonra, çıkacak olan sihirbaz yardımı ile daha sonra değiştirmek mümkündür.

- **Use array policy only**

  Bu seçenek ile Enterprise Policy çapında yapılan ayarlar ISA Server'ı etkilememektedir. Bunun sonucunda, doğal olarak ilgili kuralların yönetici tarafından oluşturulması gerekmektedir.

- **Use this enterprise policy**

  Burada önceden var olan bir Enterprise Policy var ise onu seçmek zorunludur. Bu şekilde sadece seçilen Enterprise Policy ayarları geçerli olacaktır.

- **Allow array-level access policy rules that restrict enterprise policy**

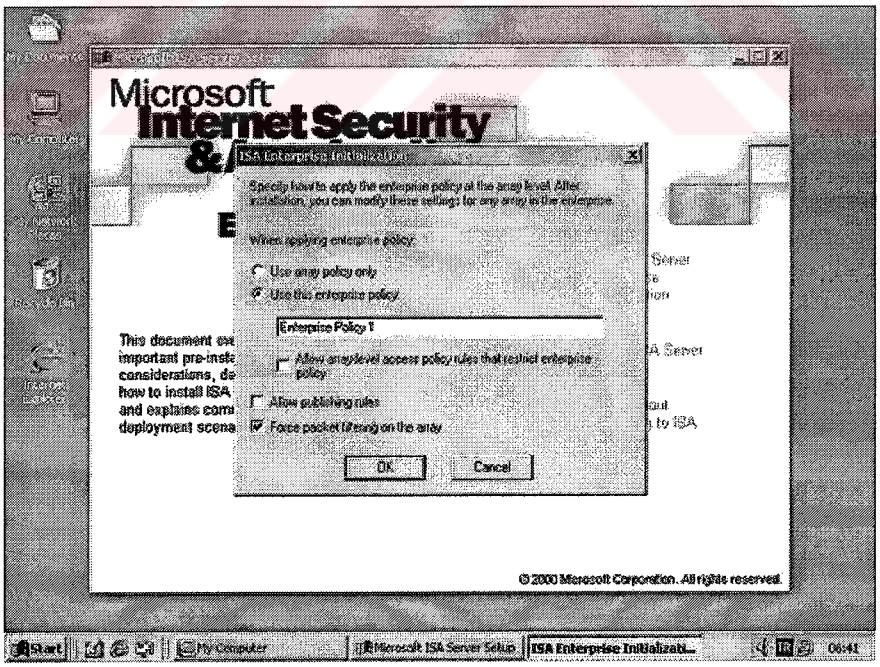
  Bu durumda Array ve Enterprise policy kombine bir şekilde çalışacaktır.

- **Allow publishing rules**

  ISA Server arkasında olan, Web Server' ların yayımlanması ile ilgilidir.

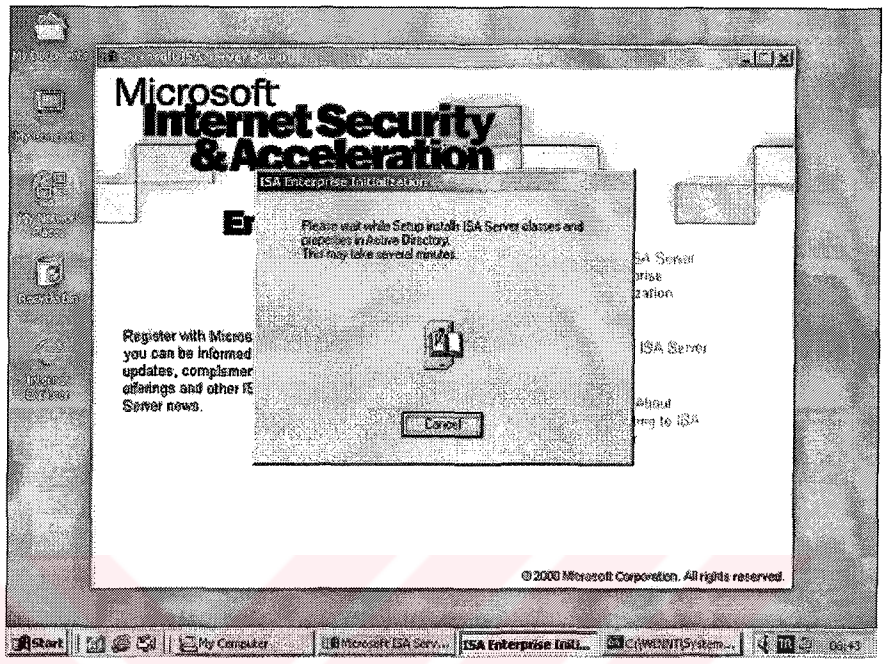
- **Force packet filtering on the array**

  İç ve dış ağ üzerindeki IP paketlerinin kontrolünü sağlamaktadır.

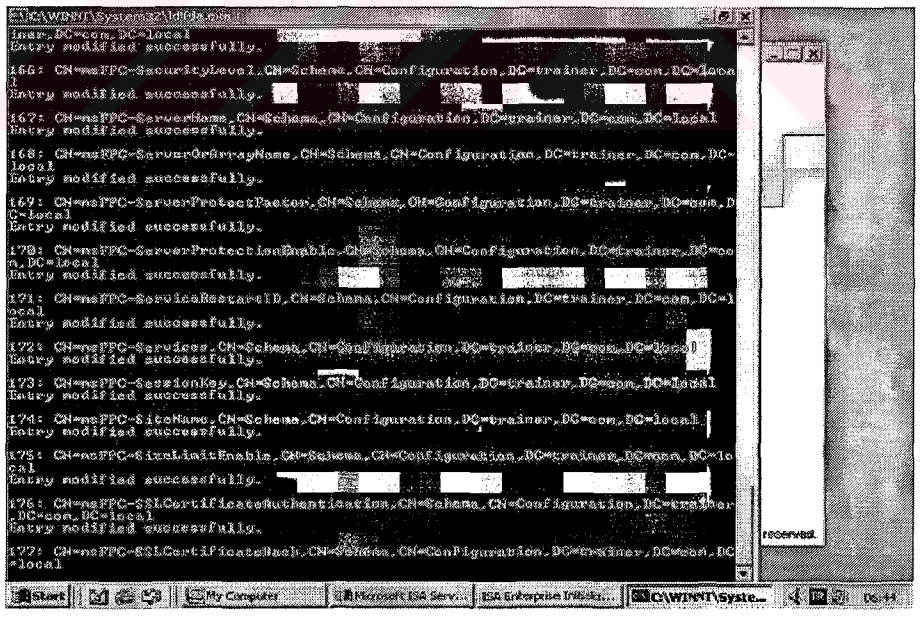


Şekil 6.5. Array ve Enterprise Policy Seçenekleri

ISA Server, Active Directory Schema üzerinde kurulum ile ilgili gerekli ayarları yapmaya başlayacaktır **(Şekil 6.6. ve Şekil 6.7.).** Burada Active Directory Schema ile ilgili güncelleme işlemleri bitinceye kadar bir süre beklemek lazımdır.

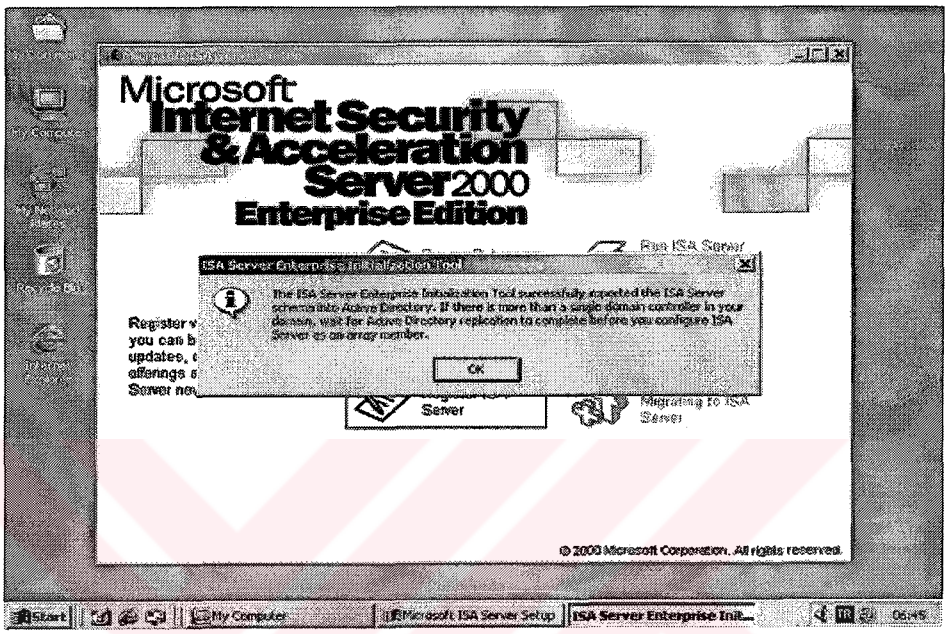


Şekil 6.6. Active Directory Schema Kurulum İşlemleri-1



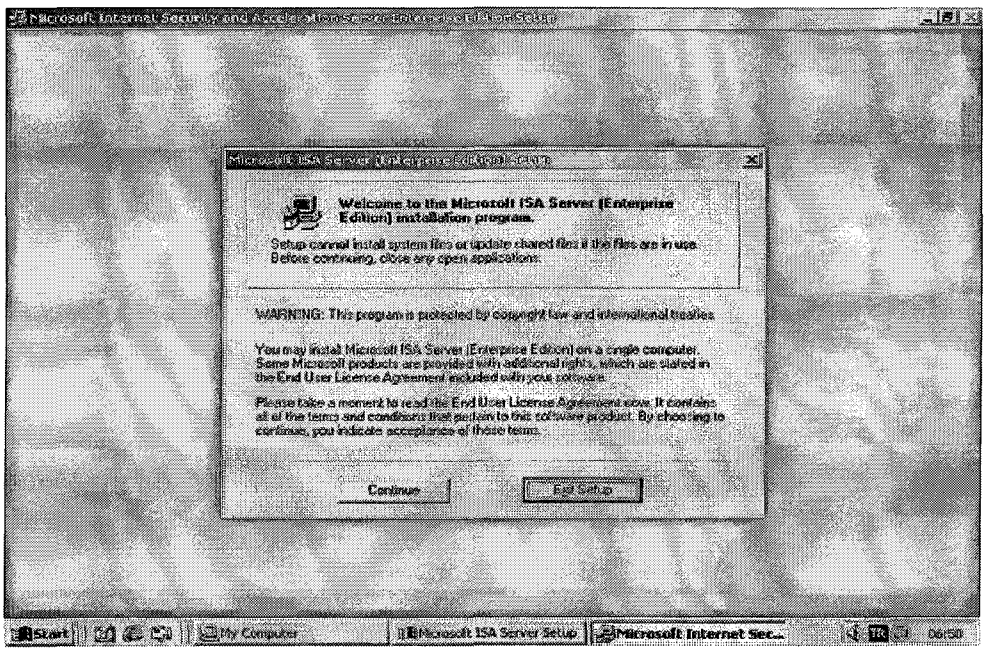
Şekil 6.7. Active Directory Schema Kurulum İşlemleri-2

Active Directory Schema ile ilgili güncelleme işlemleri bittikten sonra, işlemlerin başarı ile sonuçlandığına dair bir uyarı ekranı gelecektir. Bu ekranda, eğer birden fazla alan kontrolcüsü (Domain Controller) kullanılıyorsa, ISA Server Array konfügürasyonunu yapmadan önce Active Directory Replication operasyonunun tamamlanması için beklemek gerektiği konusunda uyarı mesajı verecektir. **(Şekil 6.8.)** "OK " tıklanır ve "Setup" bölümününe geri dönülür.



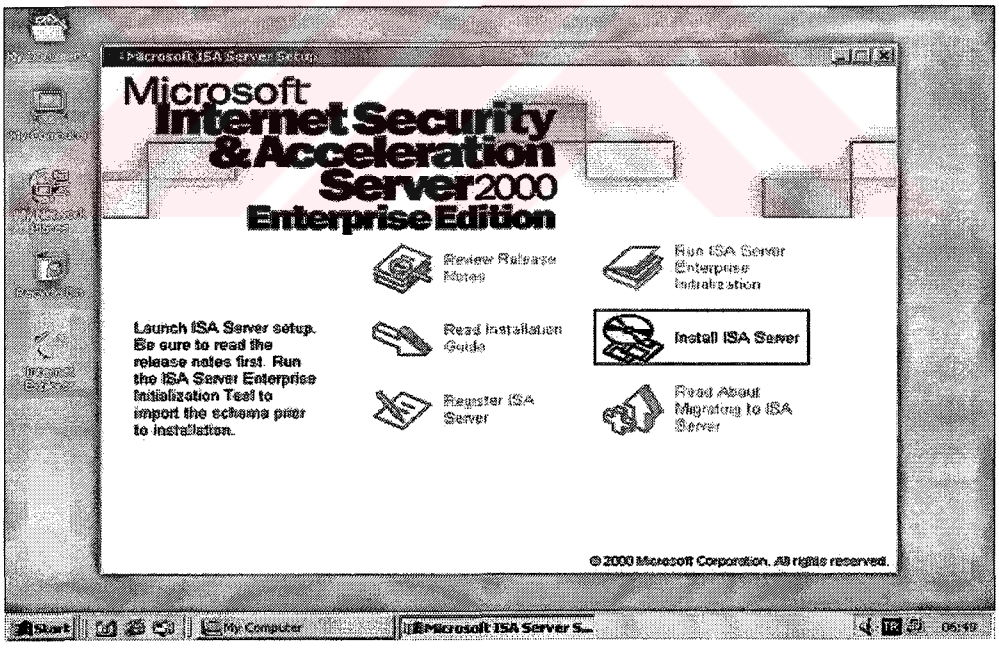
Şekil 6.8. Active Directory Replication Operasyonu Uyarı Mesajı

Bu aşamadan sonra, **Şekil 6.9'** da görülen ekran gelmelidir. **"Continue"** tıklanmadan önce, arka planda çalışan herhangi bir uygulama var ise, kapatılması faydalı olacaktır.



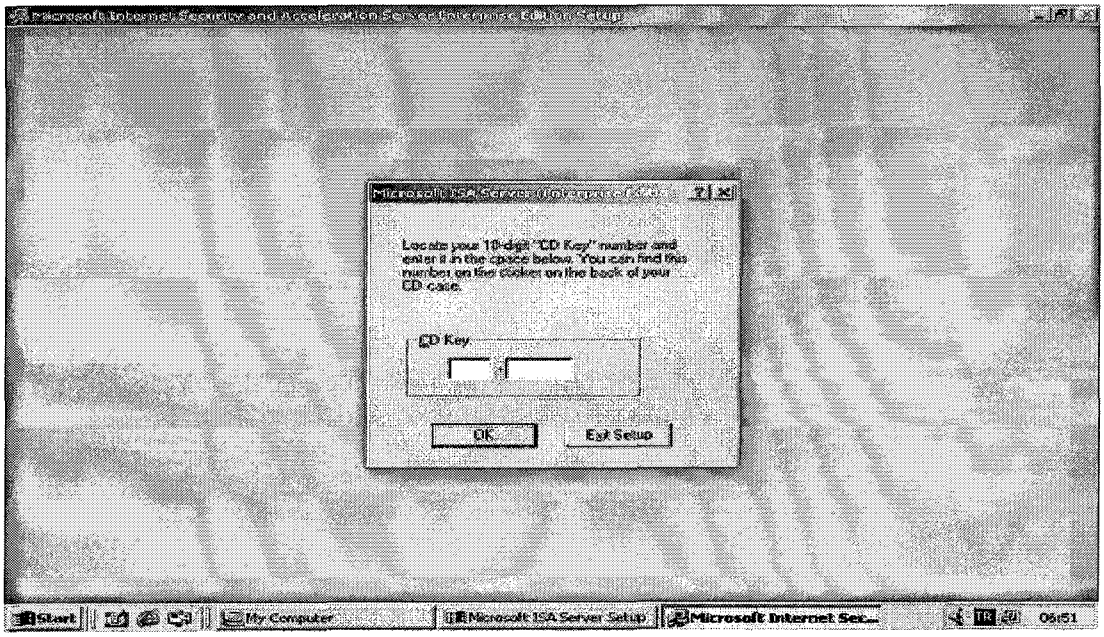
Şekil 6.9. Devam ve Kurulum' dan Çıkış Seçenekleri

"Install ISA Server" tıklanır **(Şekil 6.10.)** ve kurulum işlemi başlatılır.



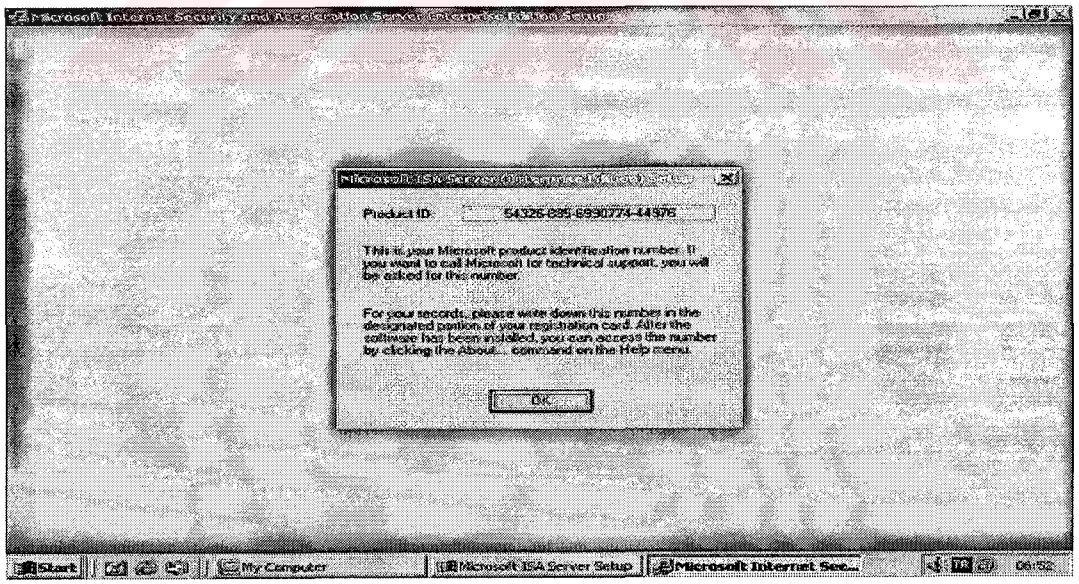
Şekil 6.10. Install ISA Server Seçeneği Görünümü

Şekil 6.11 'de ilgili **"CD Key"** in girilmesi istenmektedir. CD Key girilir ve **"OK"** tıklanır.



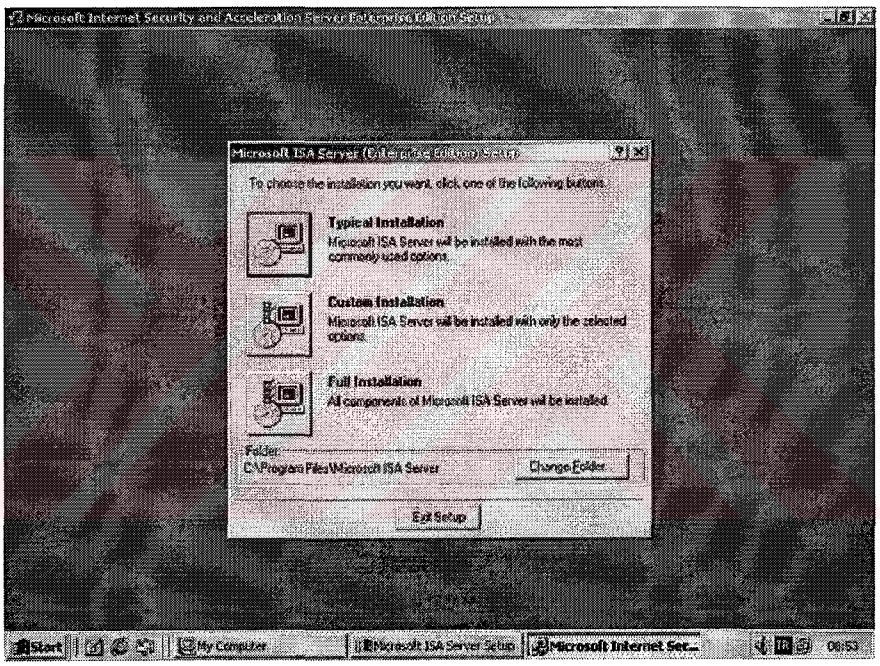
Şekil 6.11. CD Key Girilmesi İşlemi

Şekil 6.12' de görülen **"Product ID"** numarası, Microsoft' tan ürün ile ilgili teknik destek almak istenmesi durumunda, sorulacak olan numaradır. Kurulumdan sonra **"Help"** menüsünden **"About"** tıklanmak suretiyle, tekrar bu numaraya erişmek mümkündür. **"OK"** tıklanır ve sonraki ekrana geçilir.

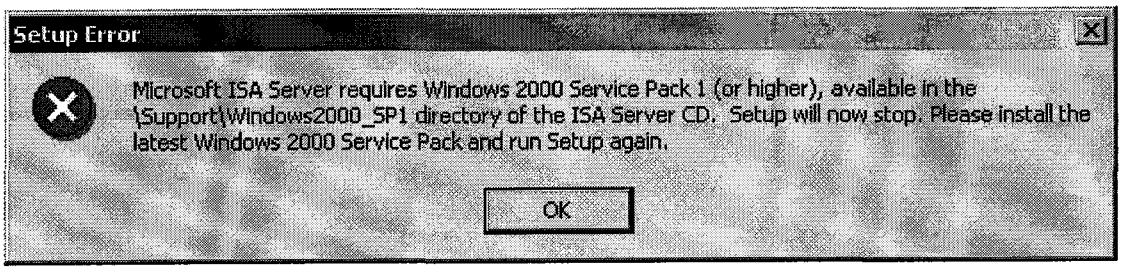


Şekil 6.12. Ürün Kimliği Numarası

Her program kuruluşunda olduğu gibi burada da programın nasıl kurmak istendiği sorulmaktadır **(Şekil 6.13.) "Typical Installation"** tıklanır. Ayrıca, **"Change Folder"** tıklanmak suretiyle programın kurulacağı disk bölümü ve dizin (directory) bilgisi değiştirilebilir. Default olarak, program **"C:\PROGRAM FILES\MICROSOFT ISA SERVER"** bölümüne kurulur. Minimum **"Windows 2000 Service Pack 1"** yaması, sunucuda kurulu olmalıdır. Eğer sunucuda Service Pack kurulu değil ise **Şekil 6.14'** de görülen hatayı almak kaçınılmazdır [19]. Bu durumda setup programı sonlanacak ve sisteme Service Pack yüklendikten sonra, yeniden Setup programının çalıştırılması gerekecektir. Eğer durum itibari ile son sürüm Service Pack temin edilemeyecek ise, ISA Server CD' si içerisinde bulunan Windows 2000 Service Pack 1' i yükleme şansı da mevcuttur
(X:\support\Windows2000_SP1).

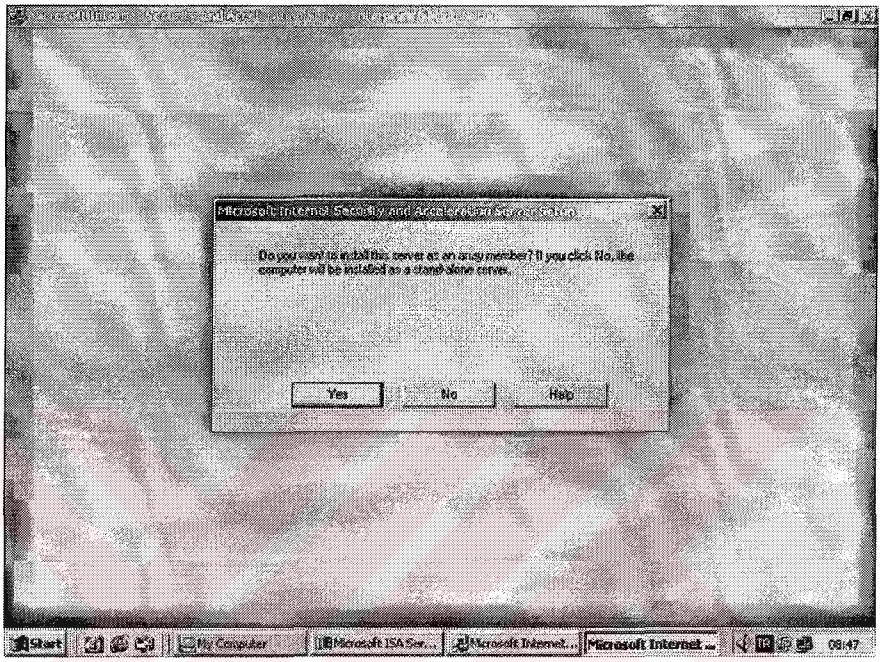


Şekil 6.13. Kurulum Seçenekleri



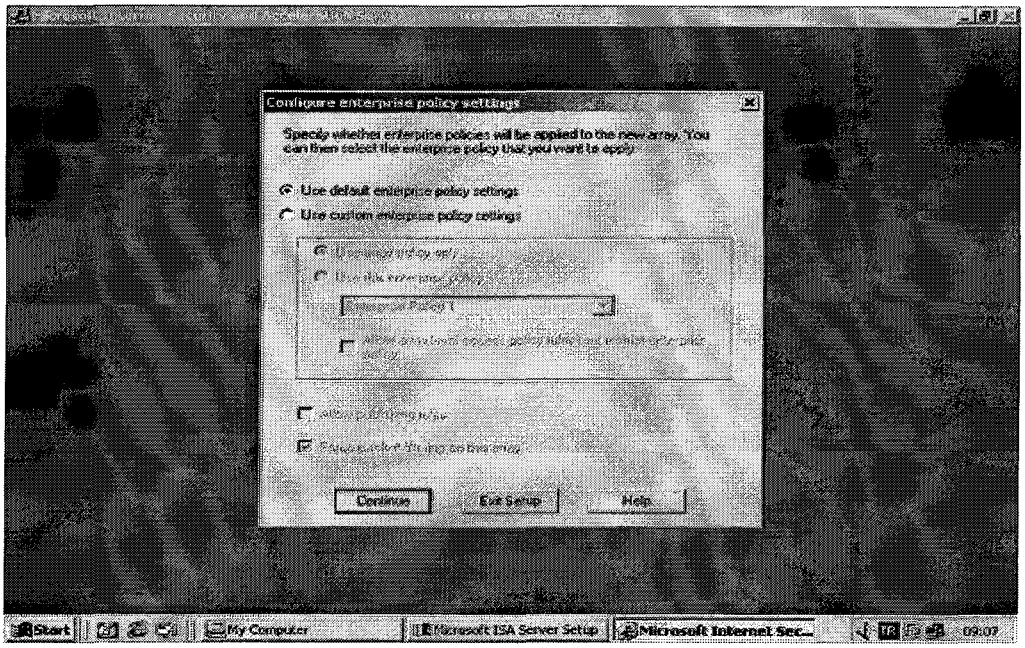
Şekil 6.14. Service Pack 1 veya Daha Üst Versiyonu' nun Kurulması Gerektiği Uyarısı

Şekil 6.15' de görülen ekranda, kurulacak ISA Server' ın bir **Array** üyesi olup olmadığı sorulmaktadır. Önceden var olan bir **Array' e** üye yapmak için **"Yes"** tıklanmalı, **"No"** tıklandığında, ISA Server Stand-Alone Server olarak kurulacaktır. Stand-Alone Server olarak kurulan ISA Server, **Array** üyesi olmak üzere, daha sonra upgrade edilebilmektedir. Daha önceden mevcut bir **Array** olmadığı için burada **"Yes"** tıklanır ve oluşturulacak olan yeni **Array** için bir isim girilmesi sağlanmalıdır. **Array** ismi girilir ve **"OK"** seçilir.



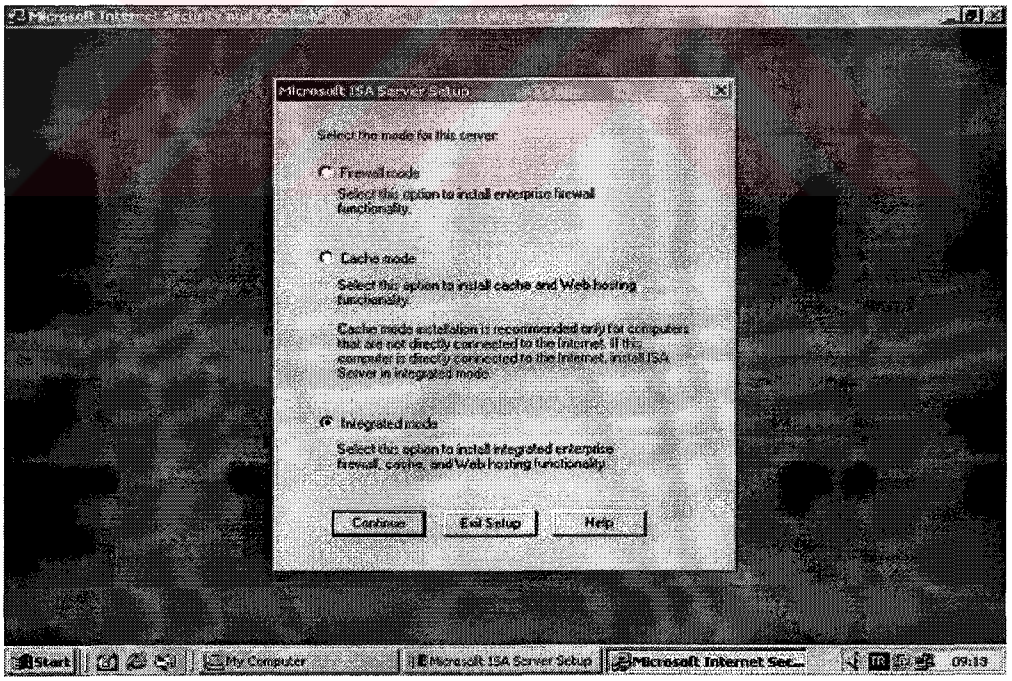
Şekil 6.15. ISA Sunucu' nun Bir Array Üyesi Olup Olmadığının Sorulması

Şekil 6.16' da görülen ekranda, **"Enterprise Policy"** ayarlarının yapılması istenmektedir. Önceden var olan **"Policy"** ayarlarları olmadığı için, **"Use Default Enterprice Policy Settings"** seçildikten sonra, **"OK"** tıklanır.



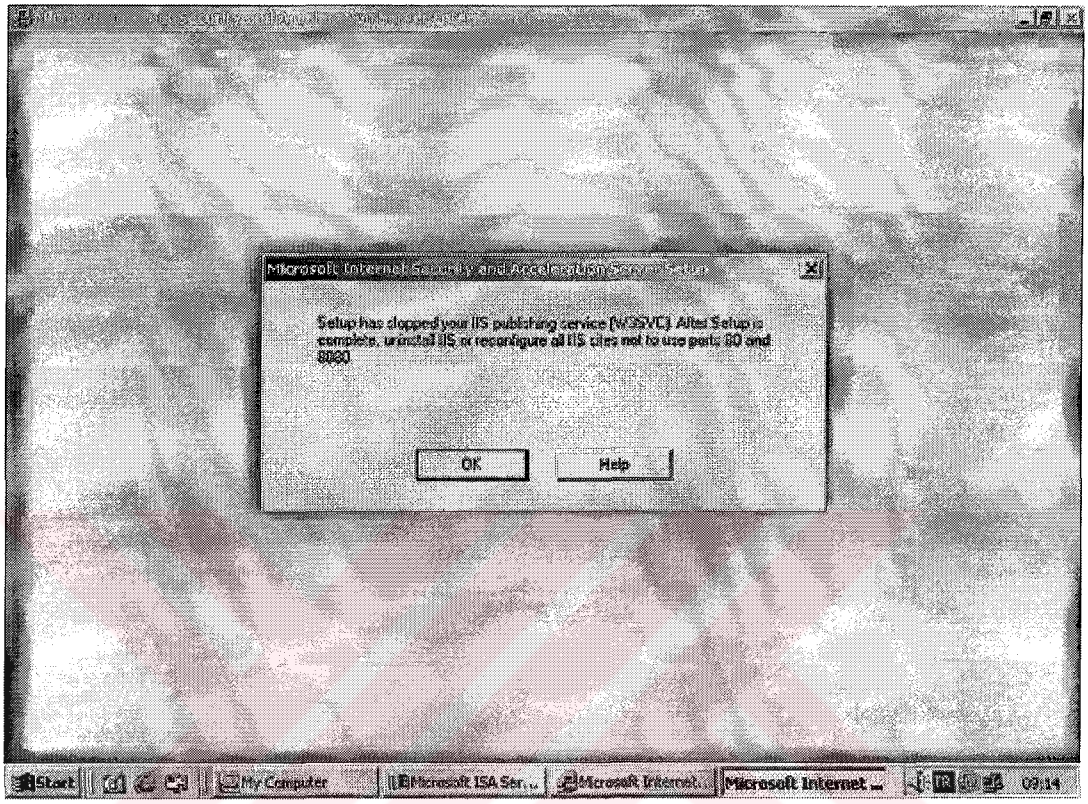
Şekil 6.16. Enterprise Policy Ayarları

Sıradaki pencere, ISA Server için mod seçimi ekranıdır. **"Integrated"** mode şeçilip, **"Continue"** denilir **(Şekil 6.17.).**



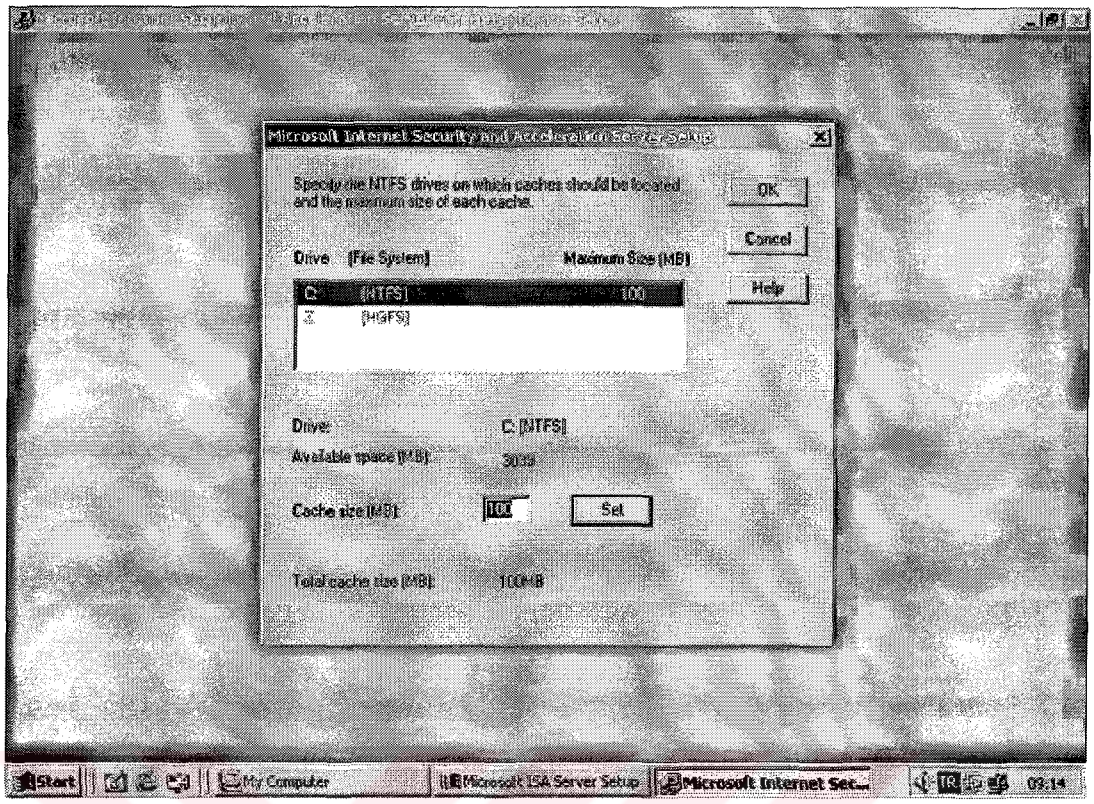
Şekil 6.17. ISA Sunucu için Mod Seçimi Ekranı

Setup programı geçici olarak **"IIS (W3SVC)"** servisini durduracağı hakkında bir uyarı verecektir **(Şekil 6.18.).** Ayrıca IIS kullanılıyorsa, kurulumdan sonra, IIS sitelerinin port ayarlarını **"80 ve 8080"** kullanılmayacak şekilde yapılandırmak gerektiği hakkında da bir uyarı vardır. **"OK"** tıklanır.



Şekil 6.18. IIS Servislerinin Geçici Olarak Durdurulması

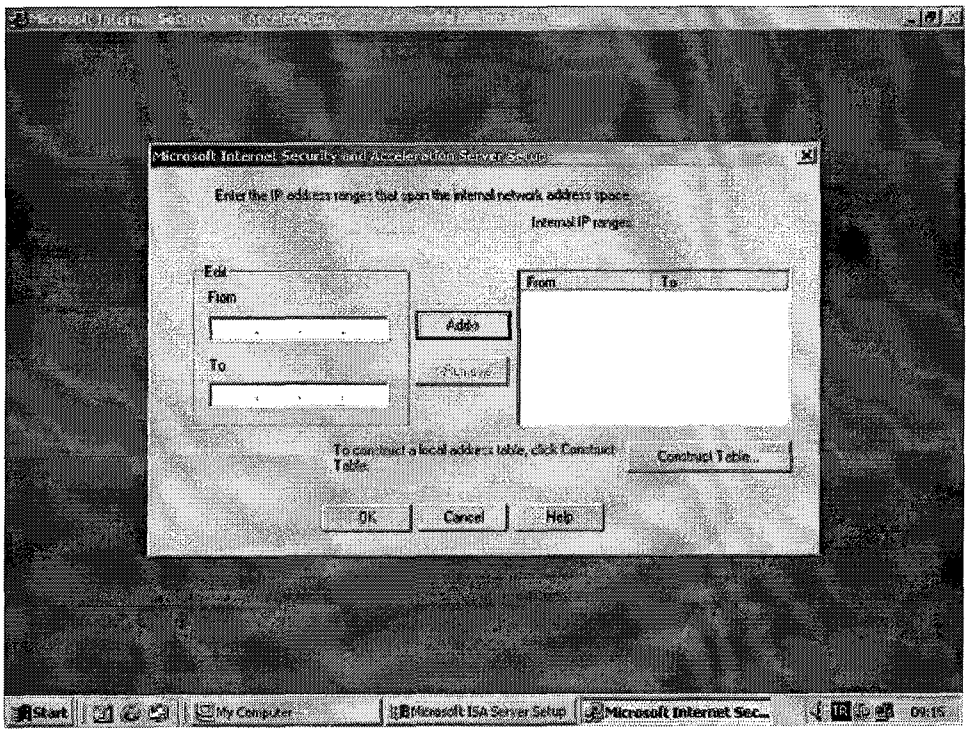
Şekil 6.19' da, ISA Server Cache ayarları hakkında bilgiler vermektedir. Default olarak ISA Server kendisi, 100 MB olarak Cache boyutunu ayarlamaktadır. İstenilirse, bu bölümde Cache dosyası için ilgili disk bölümünü ve dosya büyüklüğünü ayarlama imkanı mevcuttur [8].



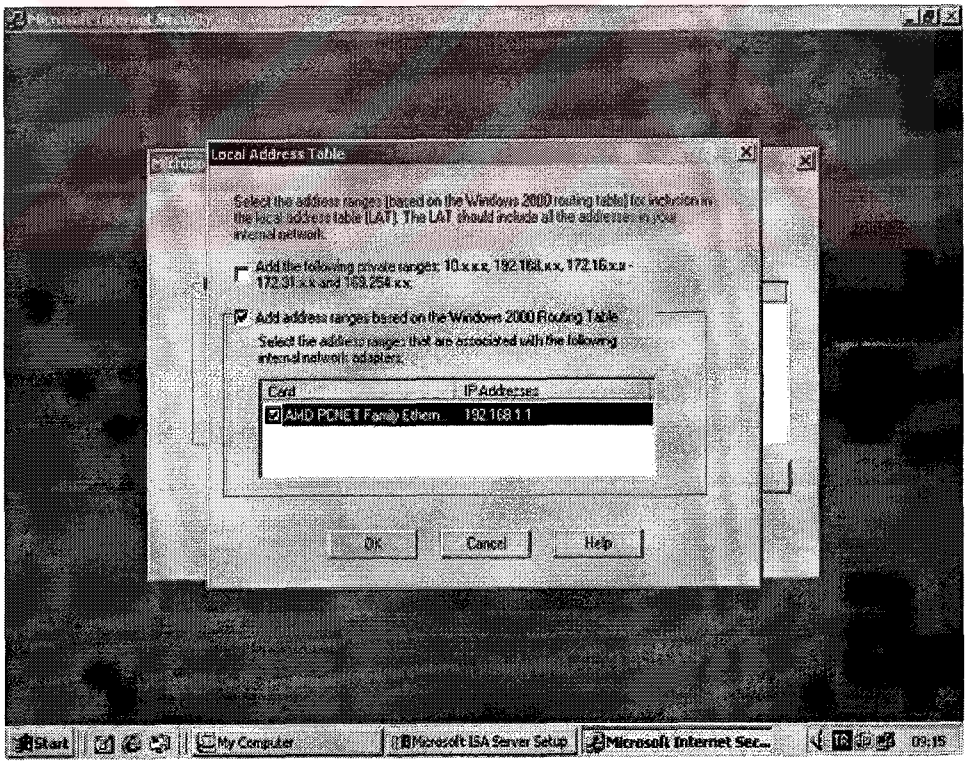
Şekil 6.19. ISA Sunucu Cache Bellek Ayarları

Bir sonraki şekilde LAT (Local Address Table) ekranı görülmektdir. Burası oldukça önemlidir, zira yanlış yapılandırılan bir LAT konfügürasyonu, istenmedik sorunlara yol açabilmektedir. Buradaki temel mantık, ISA Server' ın iç ve dış ağ' ı bilecek şekilde tanıtma işlemidir. Yani, burada yapılması gereken iç ağ' a bakan ethernet kartının IP aralıklarını uygun şekilde girmektir. İstenirse manuel olarak da **"Construct Table"** tıklanarak, bu aşama daha güvenilir gerçekleştirilebilir.

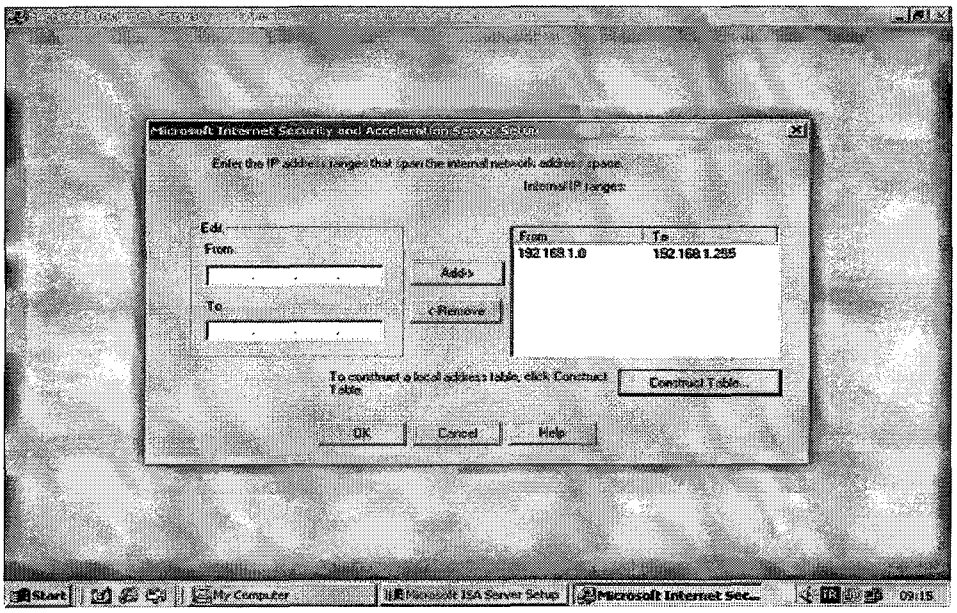
Gelen ekranda seçilmesi gereken Ethernet kartı, iç ağ' da kullanılan Ethernet kartı olmalıdır. Kesinlikle dış ağ' da kullanılan Ethernet kartı seçilmemelidir. Zaten LAT konfügürasyonu doğru yapılmış bir ISA Server, kurulumdan sonra Internet' e çıkamaz durumda olacaktır **(Şekil 6.20, Şekil 6.21, Şekil 6.22).**



Şekil 6.20. Yerel Adres Tablosu Ekranı

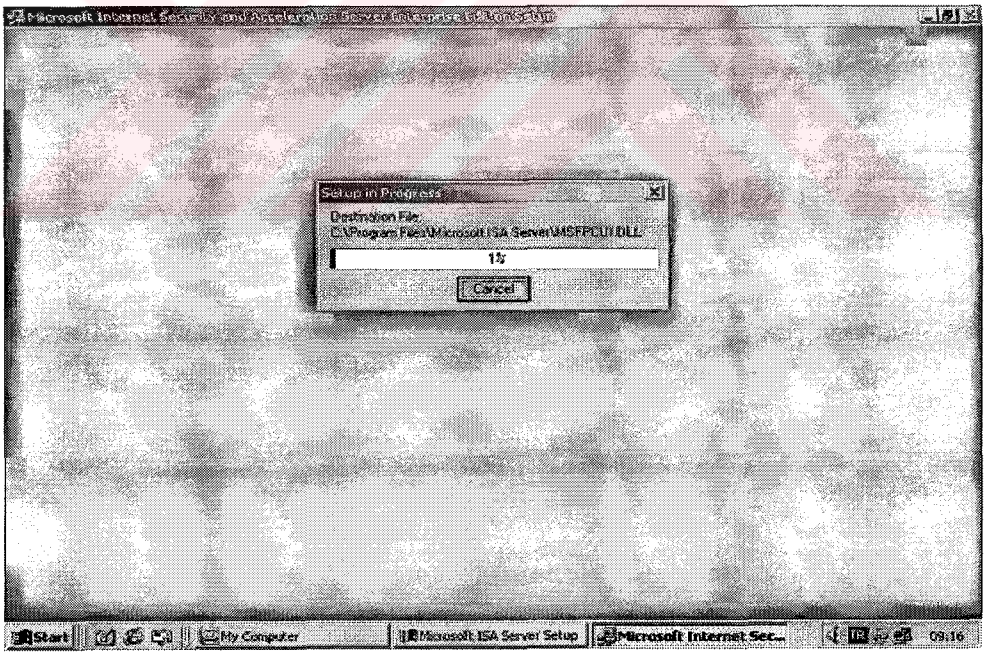


Şekil 6.21. İç Ağ' a Bakan Ethernet Kartının Seçilmesi



Şekil 6.22. LAT (Local Adres Table) Konfügürasyonun Bitirilmesi

LAT konfügürasyonu bittikten sonra, ISA Server ile ilgili dosyalar sunucuya kopyalanmaya başlayacaktır **(Şekil 6.23.).**

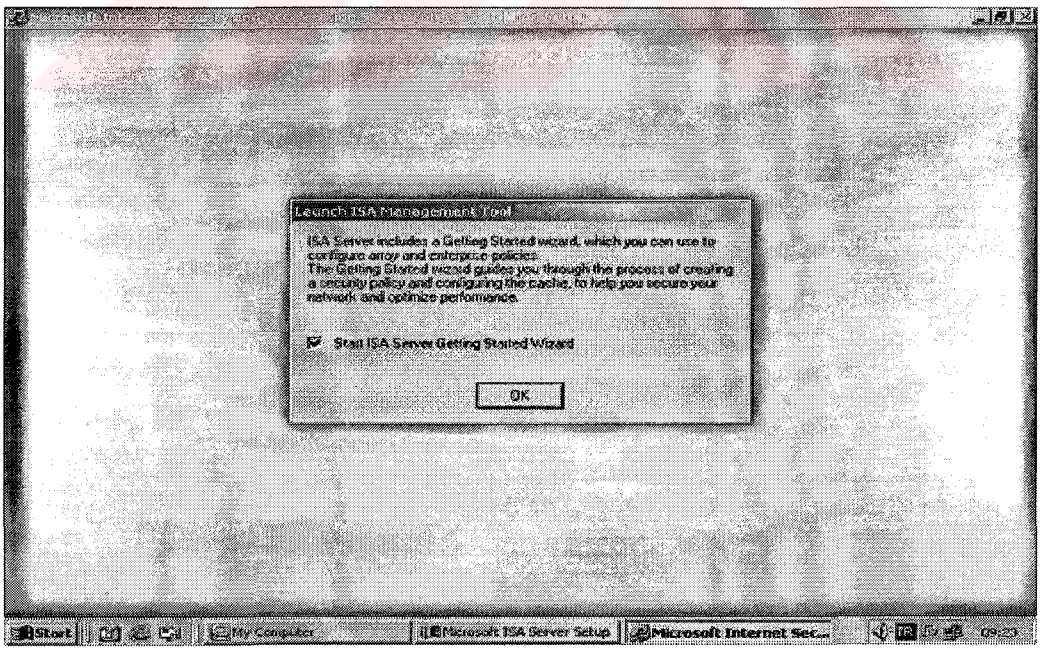


Şekil 6.23. ISA Sunucu ile İlgili Dosyaların Sunucuya Kopyalanması

Kopyalama işlemi bittikten sonra, setup programı tarafından önceden durdurulmuş olan servis /servisler tekrar başlatılmaktadır **(Şekil 6.24.).**

Şekil 6.24. IIS Servislerinin Tekrar Başlatılması

Aşağıdaki şekilde görüldüğü gibi **"Start ISA Server Getting Started Wizard"** kutucuğu seçilerek, kurulumdan sonra ISA Server konfügürasyonu hakkında bir sihirbazın yardımcı olması sağlanabilir **(Şekil 6.25.).**



Şekil 6.25. ISA Sunucu Yapılandırılması Hakkında Sihirbaz Kullanma Seçimi

ISA Server'ın kurulması işlemleri sorunsuz bir şekilde tamamlanmıştır **(Şekil 6.26.).**

Şekil 6.26. Kurulum' un Tamamlandığına Dair Uyarı Mesajı

6.4.3.1. ISA Sunucu' ya Kurulan Kritik Hotfix' ler ve Yama Programları

- ISA Server 2000 Service Pack-2 **(isasp2-ENU.exe)**
- ISA Server 2000 Feature Pack-1 **(isafp1.exe, isafp1sd.exe, isafp1ur.exe)**
- ISA Server 2000 Hotfix for FTP Client Invalid PORT Command **(ISA2000-KB816459-x86.exe)**
- ISA Server 2000-Vulnerability in H.323 filter can Cause Remote Code execution **(ISA2000-KB816458-x86.exe)**
- ISA Server 2000 Security Patch for Unchecked Buffer in Gopher Protocol Handler **(isahf177.exe)**
- ISA Server 2000 Hotfix for Rules Engine and Potential Web Proxy Service Crash **(isahf174.exe)**
- ISA Server 2000 Security Patch for Winsock Proxy Service **(isahf257.exe)**
- ISA Server 2000 Security PAtch for DNS Intrusion Detection filter **(isahf256.exe)**

6.4.4. ISA Sunucu İstemci (Client) Ayarları

Üç farklı şekilde, istemcileri ISA Server üzerinden Internet' e çıkarmak mümkündür.

a) Web Proxy İstemci

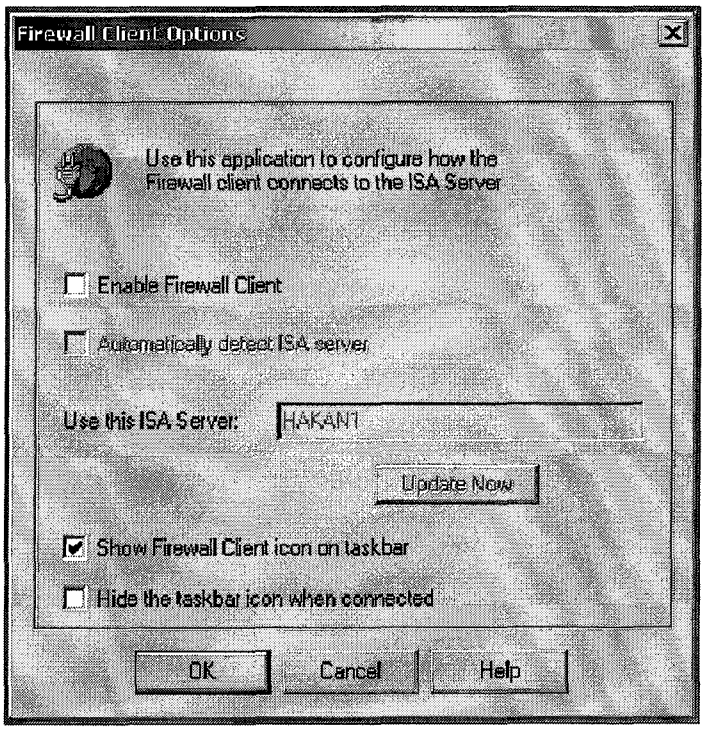
Önce, İstemci (Client) üzerindeki Internet Explorer ayarlarında proxy ayarları yapılır. Internet Explorer' da **Tools** menüsü açılır ve **Internet Options** sekmesi tıklanır. En altta görülecek olan **LAN Settings** tıklanır. **Use a proxy server for your lan** kutucuğuna **ISA Server adı** girilir, aynı yerde olan port bölümüne ise, **8080 (default)** portu girilir. Bu şekilde yapılan bir konfügürasyonda kullanıcı bazında kısıtlama yapılabilir, fakat ISA Server raporlarında kullanıcı bazında bilgi görülemez [8].

b) SecureNAT İstemci

İstemci (Client) ağ özelliklerinde, default geçityolu (gateway) olarak ISA Server' ın içe bakan ethernet kartının IP numarası girilir. Bu modda, herhangi bir kısıtlama yapmak mümkün değildir. Eğer tüm istemciler (client) bu şekilde konfigüre edilmek isteniyorsa, DHCP üzerinden default gateway adresi girilmesi ve istemcileri otomatik IP adresi alacak şekilde yapılandırmak, olası bir yanlışlığı tamamen ortadan kaldıracaktır.

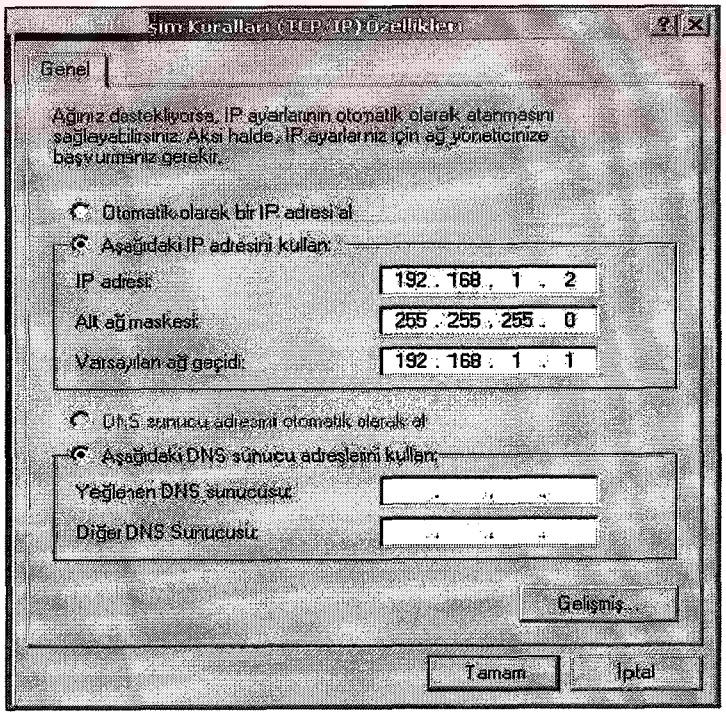
c) Firewall İstemci

Bu yöntem, tavsiye edilen metoddur. Bunun için, istemci bilgisayar üzerine basit bir program kurmak gerekmektedir. İlgili program ISA Server üzerinde, ağ üzerinden ulaşılabilecek şekilde paylaştırılmış olarak bulunmaktadır. Bu şekilde authentication, yani kullanıcı bazında kimlik doğrulama ve ilke (policy) ayarları geçerli olmaktadır. İlgili raporlarda kullanıcı bazında bilgiler görmek mümkün olabilmektedir. Programı kurmak için ağ üzerinden **\\Server\Mspclnt\setup.exe** çalıştırılır **(Şekil 6.27.).**

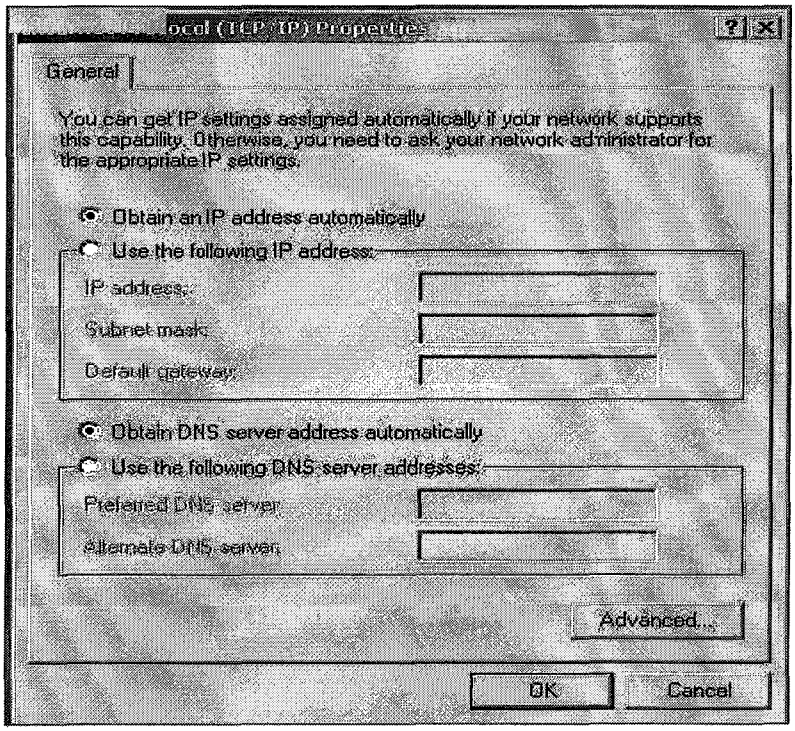


Şekil 6.27. Firewall İstemci programı

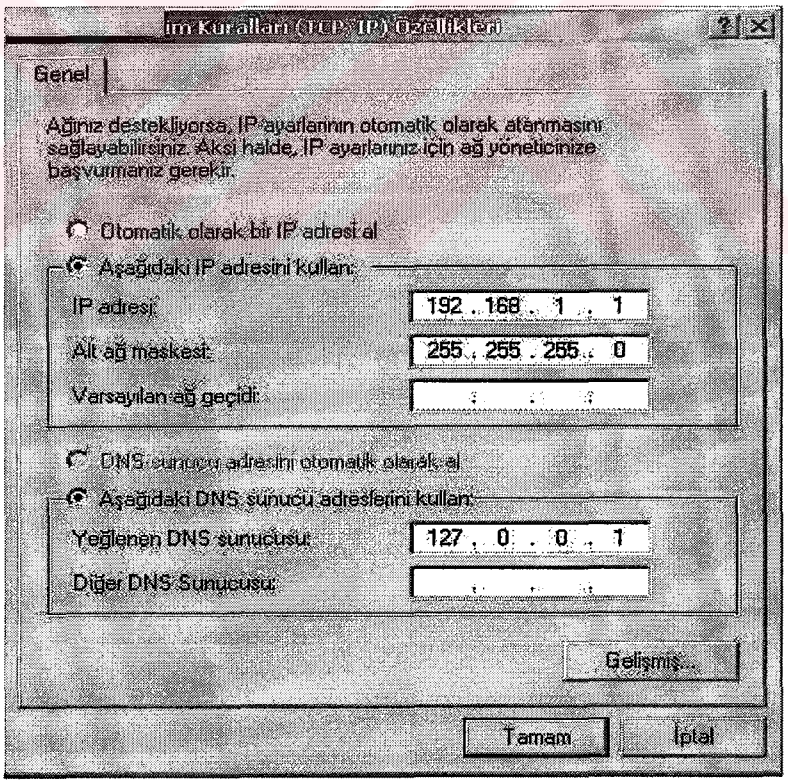
Aşağıdaki verilen şekillerde, ISA sunucu üzerindeki Ethernet kartlarında ve istemci makinede yapılan IP adres ayarları görülmektedir (**Şekil 6.28., Şekil 6.29., Şekil 6.30.**).



Şekil 6.28. İstemci Makinedeki IP Yapılandırılması

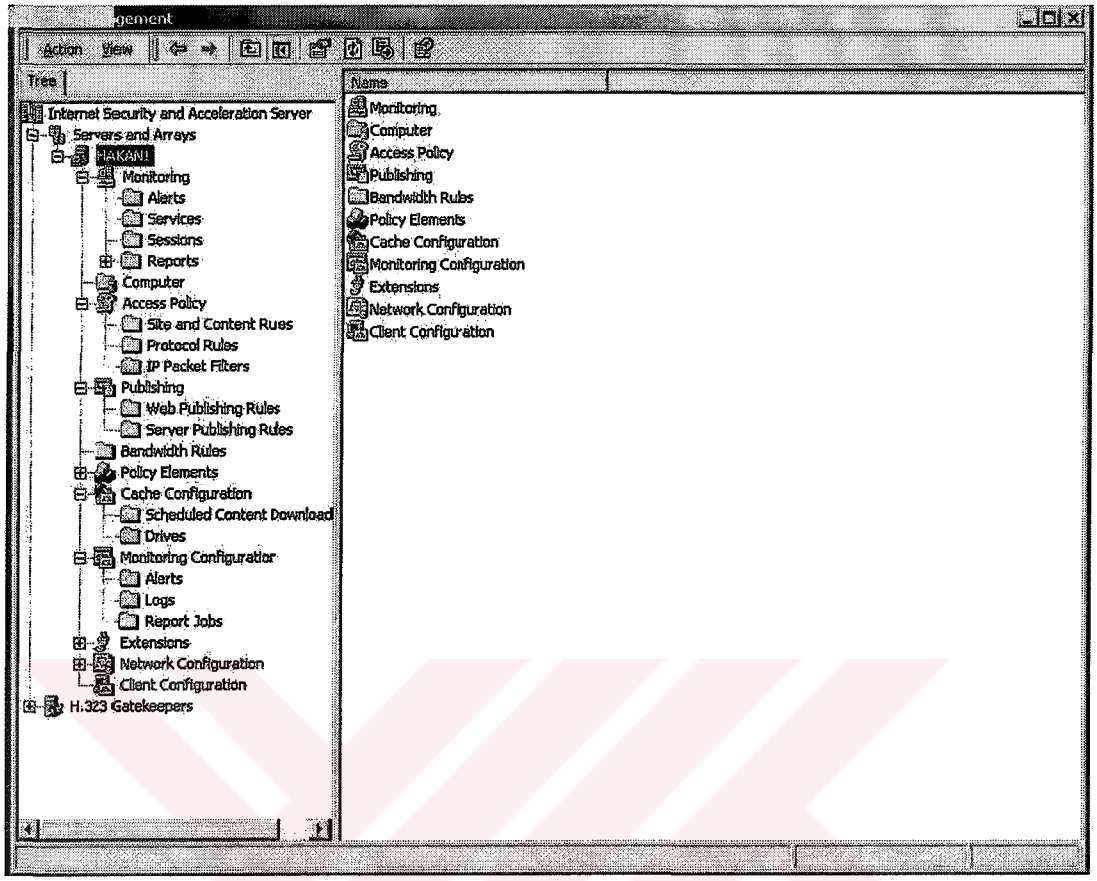


Şekil 6.29. Sunucu Üzerindeki Dış ağ' a Bakan Ethernet Kartı' nın IP Yapılandırılması



Şekil 6.30. Sunucu Üzerindeki İç ağ'a Bakan Ethernet Kartı' nın IP Yapılandırılması

6.4.5. ISA Management Kullanımı



Şekil 6.31. ISA Yönetim (management) Programı

ISA yönetim (management) programı kullanılarak, oluşturulan güvenlik duvarının yapısı ile ilgili düzenlemeler yapılabilmektedir. Ön bellek konfügürasyonu, ağı izleme (uyarılar, kayıtlar ve işler), iç ve dış ağa bakan ethernet kartlarının adreslerinin değiştirilebilmesi, sunucu üzerinde web yayımlama, site ve içerik kurallarıyla ilgili ayarlar, ağ üzerinde açılan oturumları takip etme, paket filtreleme işlemleri, istemci bilgisayarın yapılandırılması gibi birçok uygulama bu kullanışlı program aracılığıyla gerçekleştirilebilmektedir.

7. GÜVENLİK DUVARI UYGULAMASI-II

7.1. Giriş

Bu bölümde, açık anahtar şifreleme yöntemlerinden olan, RSA ve Eliptik eğri algoritmalarının yapısı ile ilgili gerekli bilgiler verildikten sonra, gerçekleştirilmiş olan nesne tabanlı uygulama programı tanıtılacaktır.

7.2. RSA Algoritması

1976 yılında Stanford Üniversitesinden Diffie ve Hellman adlı iki araştırmacı, farklı bir şifreleme sistemi önermişlerdir. Bu sistemde bir tane şifreleme için (encryption key) ve bundan farklı olarak bir tanede şifre çözmek için (decryption key) anahtar bulunmaktadır ve decryption key encryption key' den elde edilmektedir.

7.2.1. RSA Algoritmasının Önemli Özellikleri

RSA' nın yasal kullanımı ile kolayca hesaplanabilenler;

- Birbirine uyan genel (public) / özel (private) anahtar çifti oluşturulabilir.
- Eğer genel anahtar (public-key) varsa, şifreleme (encryption) ve imza onaylama (signature verification) işlemleri yapılabilir.
- Eğer özel (private) anahtar varsa, deşifreleme (decryption) ve imzalama (signing) işlemleri yapılabilir.

RSA' nın yasalara aykırı kullanımı ile hesaplaması çok zor olanlar;

- Public key varken, private key' in oluşturulması.
- Private key yokken, şifreli mesajın çözülmesi.

RSA şifreleme algoritmasının güvenli olması şu şekilde açıklanabilir:

Bu algoritmaya zarar vermek için bilinen en etkin yol, N' in asal çarpanları olan P ve Q nun bulunmasıdır. Ancak P ve Q çok büyük asal sayılar olduğundan ötürü, bulunmaları neredeyse imkansızdır. Ayrıca public key {E,N} belli iken D yi, P ve Q olmadan bulmak çok zordur. RSA açık anahtarlı şifreleme algoritması kullanılarak, çeşitli anahtar uzunluklarında anahtarlar oluşturulmuş ve şifreleme işlemleri gerçekleştirilmiştir. Ayrıca anahtar oluşturma süreleri ve şifreleme süreleri **Tablo 7.1.**' de gösterilmiştir. Test süreleri uygulamanın Pentium 4

1.7Ghz Cpu' ya sahip bir bilgisayarda çalıştırılmasıyla elde edilmiştir. Uygulamanın gerektirdiği güvenlik seviyesine bağlı olarak kullanılacak bit sayısı ayarlanabilir. Normal şartlarda 1024 bitlik anahtar kullanarak şifreleme sistemi oluşturmak yeterli güvenliği sağlamaktadır.

Tablo 7.1. RSA Algoritmasında Farklı Bit Uzunluklarında Anahtar Oluşt. ve Şifreleme süreleri

Bit Sayısı	*Anahtar Oluşturma Süresi (saniye)*	*Şifreleme Süresi (saniye)*
64	*0.021*	*0.011*
128	*0.026*	*0.013*
256	*0.083*	*0.015*
512	*0.307*	*0.018*
1024	*2.985*	*0.106*
2048	*50.432*	*0.766*
4096	*798.625*	*18.687*

7.3. Eliptik Eğri Şifreleme Algoritması

Açık anahtarlı kriptografi kullanan standartların ve ürünlerin hemen hemen hepsi, şifreleme ve dijital imza için RSA kullanmaktadır. RSA` nın güvenli kullanımı için, çalışılan bit uzunlukları zaman içerisinde büyümüş ve dolayısıyla RSA kullanan uygulamalar üzerine büyük bir hesapsal ağırlık getirmiştir. Özellikle büyük sayıların transferini güvenlik içinde gerçekleştirmesi gereken ticari siteler, bundan çok fazla etkilenmişlerdir. Eliptik Eğri Kriptografisi (ECC), açık anahtarlı kriptografi için öngörülmüş ve IEEE P1363 standartlarını yerine getirmektedir [9].

ECC` nin RSA` ya karşı en büyük avantajı, daha küçük bitler kullanılarak yapılan işlemlerin, RSA şifrelemede olduğu gibi yüksek güvenlik sağlayabilmesi, bunun sayesinde kullanıcıların şifreleme ve deşifreleme esnasında hesaplamalar için harcadıkları eforu azaltmasıdır. Diğer bir taraftan da, ECC kullanan ürünler kısa süre içerisinde kendisini göstermeye başlamakla birlikte, bu ürünler üzerinde yapılan güvenlik testleri, ECC` nin henüz RSA kadar yüksek bir güvenlik sağlayamadığını göstermiştir. ECC` nin matematiksel teorisinin açıklanması, RSA ya da Diffie-Hellman teorilerinin açıklanmasından daha zordur.

7.3.1. Eliptik Eğriler

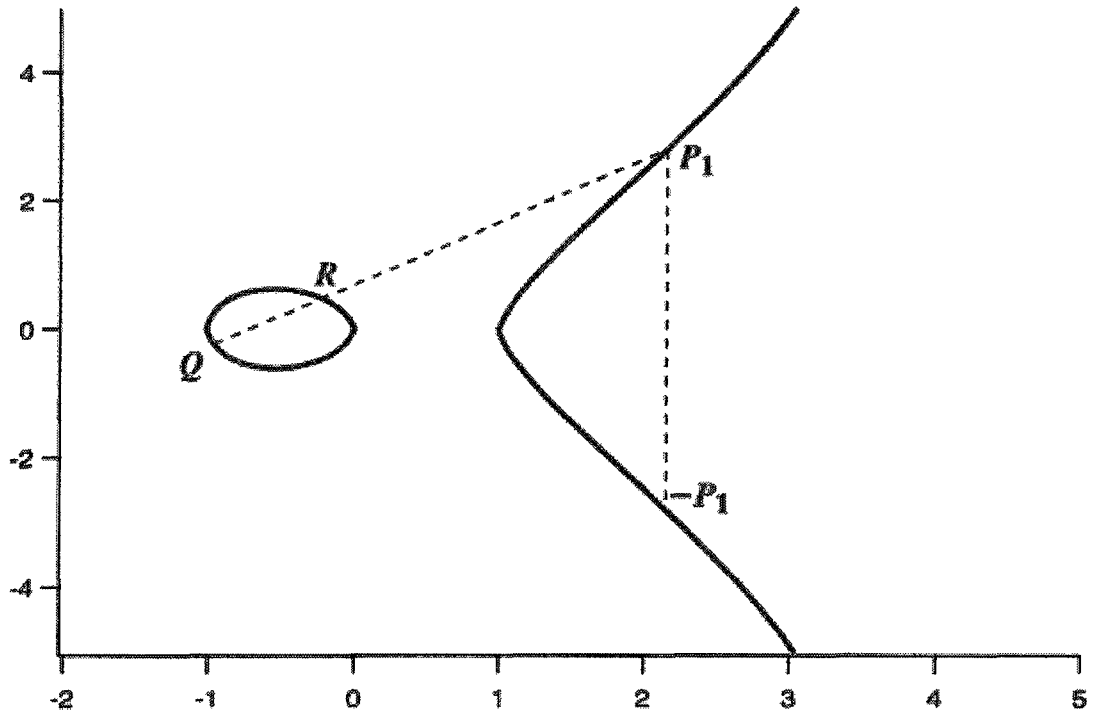
Bu eğrilerin eliptik şeklinde adlandırılmalarının sebebi, bir elipsin çemberinin hesaplanması için kullanılan kübik denkliklere benzer ifadeler ile gösterilmeleridir. Genel olarak eliptik eğriler için kübik denklemler aşağıdaki formdadır:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \qquad (7.1)$$

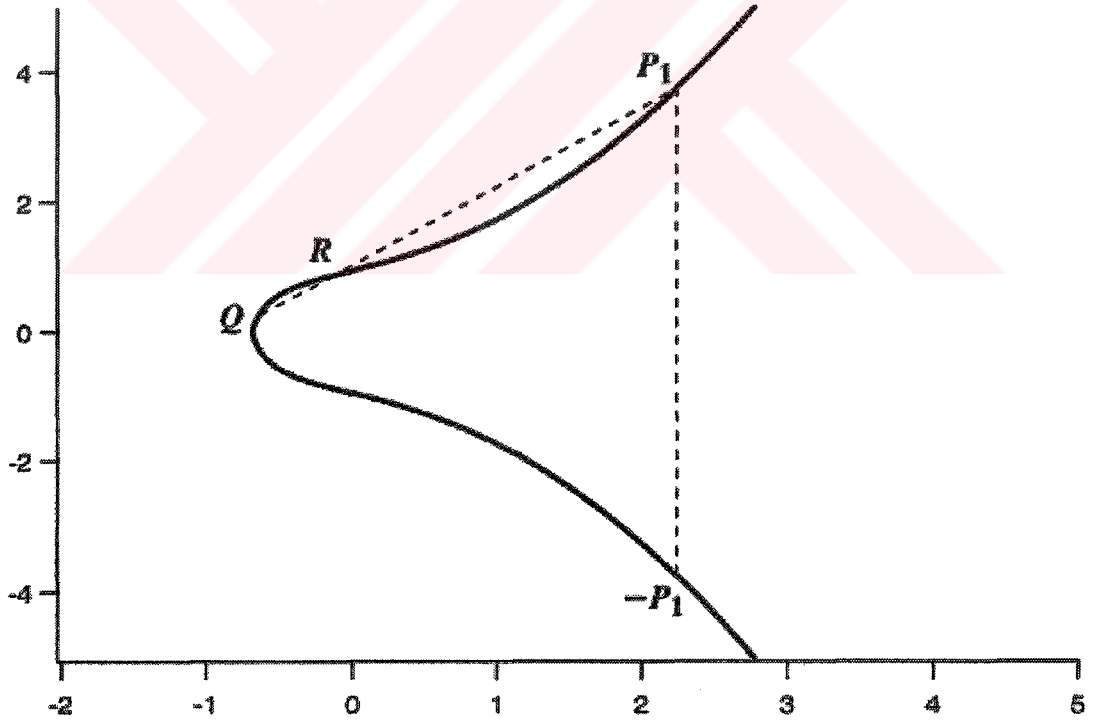
Bu denklemdeki a, b, c, d ve e sayıları reel sayılardır ve bazı basit koşulları sağlamaktadır. Ayrıca, eliptik eğrinin tanımlamasında sonsuzluk ya da sıfır nokta adı verilen bir O notasyonu vardır. En büyük dereceli üs 3 olduğundan dolayı, bu tip denklemler kübik olarak adlandırılmaktadır.

Eğer bir eliptik eğrinin 3 noktası düz bir çizgi üzerinde bulunuyorsa, bunlar O notasyonu olarak özetlenir. Bir eliptik eğri için şu kurallar tanımlanabilir:

- Eliptik eğri üzerindeki herhangi bir P noktası için, $P + O = P$ olur.
- Bir dikey çizgi, aynı x değeri için eliptik eğriyi $P_1 = (x,y)$ ve $P_2 = (x,-y)$ iki noktasında kesiyorsa, bu çizgi aynı zamanda eliptik eğriyi sonsuzluk noktasında da kesiyordur. Bu yüzden, $P_1 + P_2 + O = O$ ve $P_1 = -P_2$ olmaktadır. Böylece bir noktanın negatifi, x ekseni üzerinde aynı değeri alacak şekilde bir noktadır ve bu noktanın y ekseni üzerindeki değeri, ilk noktanın negatiflisidir **(Şekil 7.1.)**.
- X koordinatı farklı olan Q ve R noktası seçip, bu iki noktadan geçen düz bir çizgi çizildiğinde, kesişimin üçüncü noktası olan P_1 bulunur ve çok kolay bir şekilde görülebilir ki, P_1 noktası sadece bir tanedir (Eğer çizilen doğru, Q veya R noktalarından birisinden teğet geçiyorsa, bu durumda $P_1 = Q$ veya $P_2 = R$ alınır). Dolayısıyla $Q + R = +P_1$ olacaktır **(Şekil 7.1.)**.
- Bir Q noktasını çift katlı yapmak için, bir teğet çizgisi çizip, eğriyi kestiği diğer nokta bulunur. Eğer bu noktaya S denilecek olursa, $Q + Q = 2Q$ eşitliği sağlanır.



(a) $y^2 = x^3 - x$



(b) $y^2 = x^3 + x + 1$

Şekil 7. 1. Eliptik Eğri Örnekleri [9]

7.3.2. Sonlu Alanlardaki Eliptik Eğriler

P bir asal sayı ve (a, b), P` den küçük, negatif olmayan iki tam sayı olsun:

$$4a^3 + 27b^2 \pmod{p} \neq 0 \qquad (7.2)$$

Bu durumda E_p (a,b); (x,y)` nin P` den küçük negatif olmayan tam sayılar olduğu durum için, O sonsuz noktası ile beraber şu eşitliği ifade eder:

$$y^2 \equiv x^3 + ax + b \pmod{p} \qquad (7.3)$$

Örneğin, p = 23 ve eliptik eğri de $y^2 = x^3 + x + 1$ olsun. Burada, a = b = 1' dir. Bu durumda, $4 \times 1^3 + 27 \times 1^2 \pmod{23} = 8 \neq 0$, eliptik grubun mod 23` e göre durumunu göstermektedir. Eliptik grup için sadece (mod p` den dolayı), (0, 0) - (p, p) aralığında olan pozitif tamsayılar ile denklem oluşturulur [9]. **Tablo 7.2.**' de, $E_{23}(1,1)$ için O dışındaki noktalar listenmiştir. Genel olarak liste aşağıdaki yolla oluşturulmuştur:

- $0 <= x < p$ koşulunu sağlayan her x değeri için, $x^3 + ax + b \pmod{p}$ denklemi hesaplanmıştır.
- Önceki adımın her sonucu için, sonucun (mod p)` ye göre çift katlı kökü olup olmadığına bakılır, eğer yoksa bu x değeri için, $E_p$ (a,b)` nin bir değeri yoktur. Aksi takdirde, çift katlı kök koşulunu sağlayan iki adet y vardır (y` nin 0 olduğu durum haricinde). Bu (x,y) değerleri $E_p$ (a,b)` nin noktalarıdır.

Tablo 7.2. E_{23} (1, 1) Eliptik Eğrisi için Noktalar

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13,16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

E_p (a,b) için bahsedilmiş kurallar, **Şekil 7.1.**` deki geometrik şekil ile uyuşmaktadır. Kurallar, her P, Q € E_p (a,b) olacak şekilde alınan noktalar için aşağıdaki gibi gösterilebilir:

- $P+O=P$.
- Eğer P = (x,y) ise, P + (x,-y) = O olur. (x,-y) noktası, P` nin negatifidir ve $-P$ olarak gösterilir. Diyelim ki, (x,-y) **Şekil 7.1.** 'de gösterilen $E_p$ (a,b) eliptik eğrisi üzerinde bir nokta olsun. Örneğin, $E_{23}$(1, 1)` de P = (13,7) alalım. Bu durumda –P = (13,-7) olacaktır. Fakat –7 mod 23' e göre 16 ettiğinden dolayı, -P noktası aslında, yine E_{23}(1, 1)` de yer alan (13,16) noktasıdır.
- Eğer P = (x1, y2) ve Q = (x2,y2) ise ve P ≠ -Q ise, bu durumda, P + Q = (x3,y3) şu kuralla hesaplanır:

$$\left.\begin{aligned} x_3 &\equiv \lambda^2 - x_1 - x_2 (\text{mod } p) \\ y_3 &= \lambda(x_1 - x_3) - y_1 (\text{mod } p) \end{aligned}\right\} \qquad (7.4)$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & eger \quad P \neq Q \quad ise \\ \dfrac{3x_1^2 + a}{2y_1} & eger \quad P = Q \quad ise \end{cases} \qquad (7.5)$$

7.3.3. Eliptik Eğriler ile Şifreleme

ECC` deki toplama işlemi ile RSA`daki modüler çarpım işlemi ve çoklu toplama işlemi ile de, RSA` daki modüler üs alma işlemi birbirlerine çok benzemektedir. Eliptik eğriler kullanan bir kriptografik sistem oluşturabilmek için bir sayıyı iki asal çarpanına ayırmak ya da ayrık logaritma almak gibi zor bir problem bulmak gerekmektedir. Diyelim ki, P, Q € E_p (a,b) ve k < p iken, Q = kP olsun. k ve P verildiğinde Q değerini hesaplamak nispeten kolay olduğu halde, Q ve P verildiğinde k değerini hesaplamak gerçekten çok zordur [9].

7.3.4. Diffie-Hellman Anahtar Değişimi

Eliptik eğriler kullanılarak anahtar değişimi aşağıdaki şekilde yapılabilmektedir. Önce $p \approx 2^{180}$ olacak şekilde bir p asal sayısı ve **(1)** denklemindeki eliptik eğri parametreleri olan a ve b seçilsin. Bu, eliptik noktalar grubu olan E_p (a,b)` yi oluşturur. Sonrasında $E_p$ (a,b) içerisinden, başlangıç noktası (generator point) olan G= (x1,y1) seçilir. G` nin seçilmesindeki en önemli kriter, nG = O eşitliğini sağlayan en küçük n değerinin çok bir büyük bir asal sayı olması gerekliliğidir. E_p (a,b) ve G , kriptosistemin tüm katılımcılarca bilinecek parametreleridir.
Bir A ve B kullanıcısı arasındaki anahtar değişimi aşağıdaki gibi gerçekleşir :

- A, n` den küçük bir $n_A$ tamsayısı seçer. Bu $A$`nın özel anahtarıdır. Daha sonra A, $P_A=n_AG$ hesabıyla E_p (a,b)` nin bir noktası olan kendi açık anahtarını oluşturur.
- B ` de aynı metodla kendi açık anahtarı $P_B$` yi oluşturur.
- A gizli anahtarı $K= n_AP_B$ ile, B ` de gizli anahtarı $K=n_BP_A$ ile elde eder.

Üçüncü aşamadaki iki hesaplamanın sonucuda aynıdır. Çünkü,

$n_AP_B = n_A(n_BG) = n_B(n_AG) = n_BP_A$ eşitliği mevcuttur.

Bu yönteme bir atak gerçekleştirmek isteyen saldırgan, verilmiş G ve kG değerlerinden yola çıkarak, k değerini hesaplamak isteyecektir ve bu çok zordur.

7.3.5. Eliptik Eğri Şifrelemesi/Deşifrelemesi

Literatürde, eliptik eğriler yardımıyla şifreleme/deşifreleme yapan bir çok yöntem bulunmaktadır. Sistem içerisindeki ilk görev, düz yazı (plaintext) mesaj olan m` yi, bir x-y koordinatı ile belirlenmiş P_m noktası şeklinde göndermek üzere kodlamaktır (encode). Bu P_m noktası bir chipertext gibi şifrelenecek, daha sonrasında da deşifre edilecektir. Bir mesaj, x ya da sadece y koordinat noktası olarak basitçe encode edilemez, çünkü tüm olası noktalar E_p (a,b) içinde bulunmayabilir. Bu encode işlemi için de birçok yöntem mevcuttur.

Anahtar değişimi sisteminde olduğu gibi şifreleme / deşifreleme sistemi de parametre olarak bir G noktası ve bir E_p (a,b) eliptik grubuna ihtiyaç duymaktadır. Her bir kullanıcı, bir n_A özel anahtarı seçer ve $P_A = n_AG$ ile bir açık anahtar üretmektedir.

P_m gibi bir mesajı şifrelemek ve bir B kullanıcısına göndermek isteyen bir A kullanıcısı, rastgele pozitif bir k tam sayısı seçer ve C_m chipertextinin noktalarını aşağıdaki şekilde elde eder :

$$C_m = \{kG, P_m + kP_B\}$$

A kullanıcısının şifreleme esnasında, B` nin açık anahtarı olan $P_B$` den yararlandığına dikkat edilmelidir. B aşağıdaki şekilde mesajı deşifre eder:

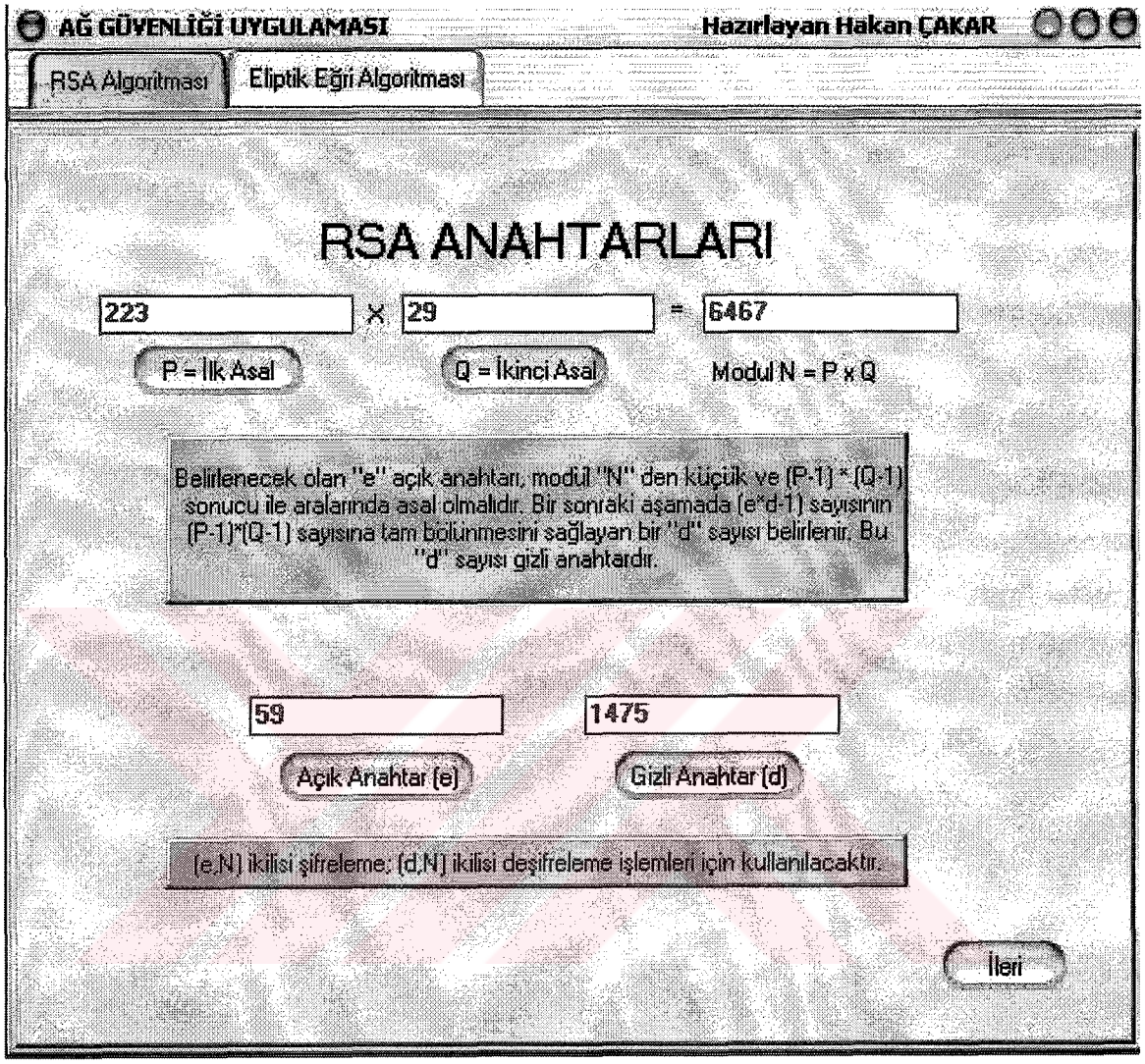
$$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m$$

A, P_m mesajını, ona kP_B ekleyerek maskelemektedir. k değerini bilmeyen kimse, A` nın uyguladığı maskeyi kaldıramamaktadır. Bunun yanında A, n_B özel anahtarını bilen bir kişinin maskeyi kaldırabilmesi için bir ipucu bırakmaktadır [9].

7.3.6. Eliptik Eğri Şifrelemenin Güvenliği

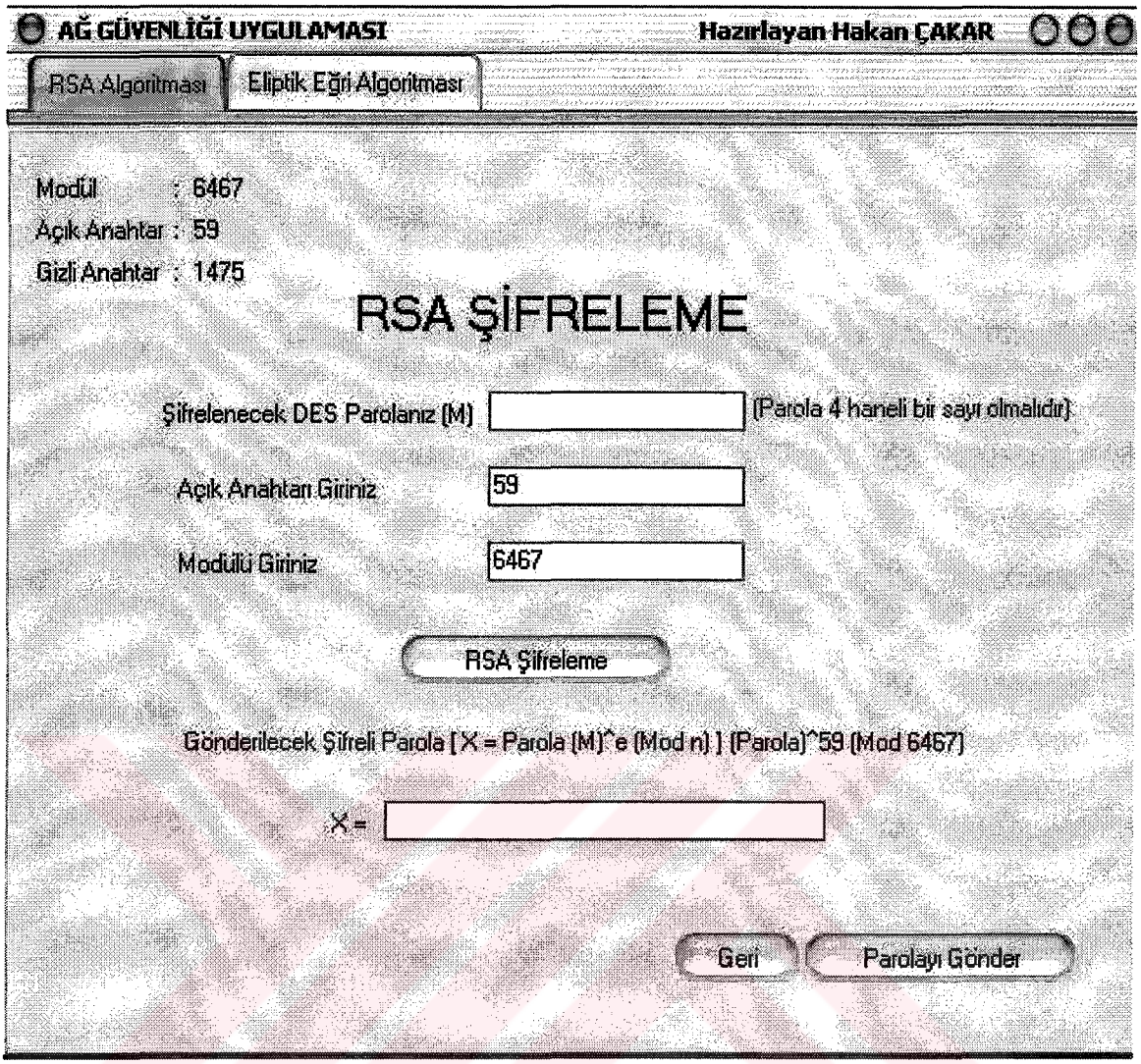
ECC`nin güvenliği, KP ve P verildiğinde k değerini elde etmenin zorluğuna bağlıdır. Bu durum, eliptik eğri logaritması problemi olarak adlandırılmaktadır. Eliptik eğri logaritması olarak bilinen en hızlı teknik, Pollard rho (rho=eşkenar dörtgen) yöntemidir.

7.4. Nesne Tabanlı Uygulama Yazılımının Çalıştırılması



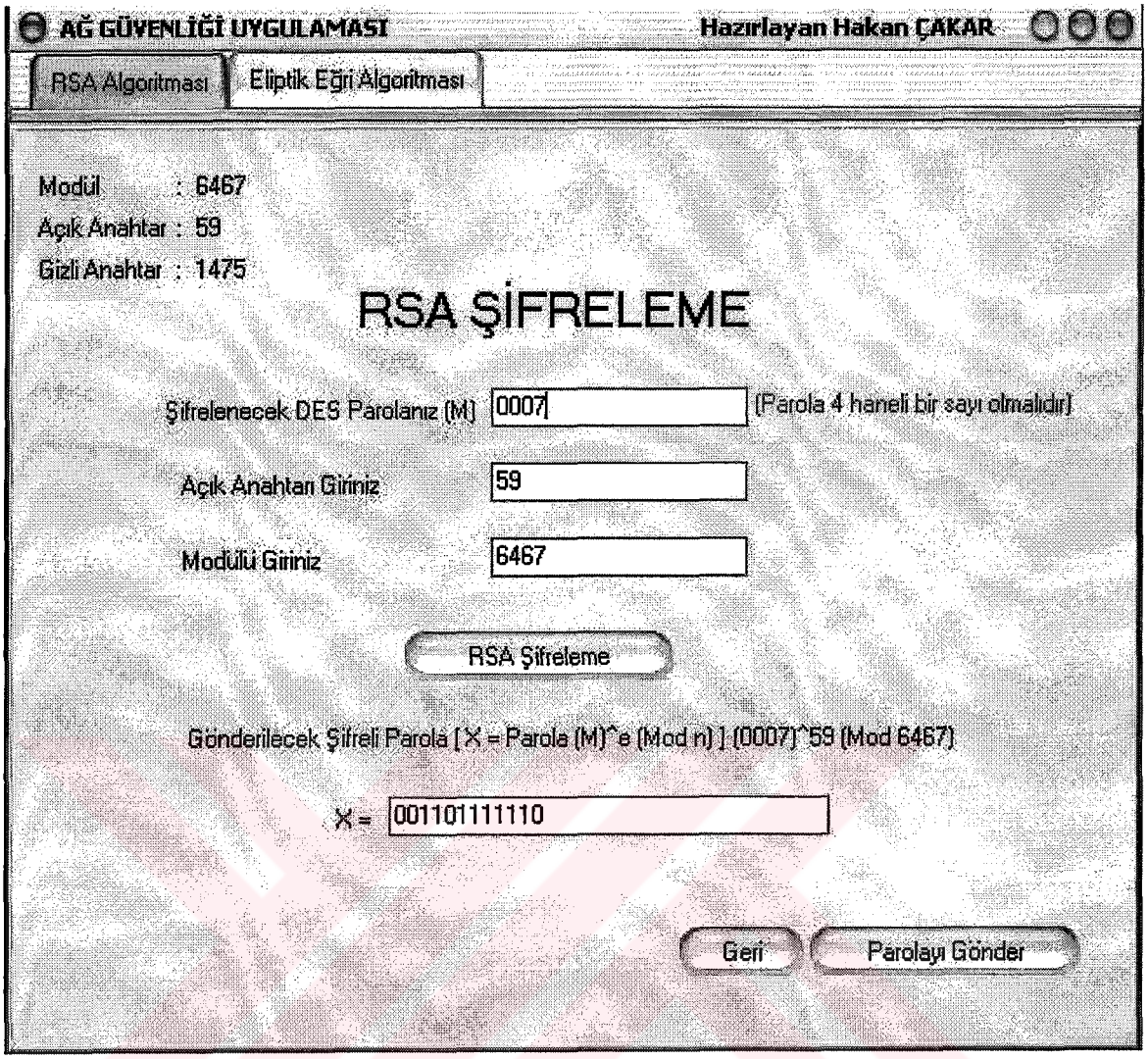
Şekil 7.2. Açık ve Gizli Anahtarların Belirlenmesi

Şekil 7.2.' de görülen ekran görüntüsünde, RSA anahtarlarının belirlenmesi işlemleri yapılmaktadır. Bunun için P ve Q asal sayıları butonlara tıklanmak suretiyle seçilmekte, daha sonra ekran görüntüsünde de verilen açıklamaya uygun, e açık anahtarı ve d gizli anahtarı tespit edilip, **İleri** butonuna tıklanmalıdır. Eğer P ve Q asal sayıları tespit edilmeden, **Açık anahtar (e)** veya **Gizli anahtar (d)** butonuna tıklanırsa, program uyarı mesajı verecektir.



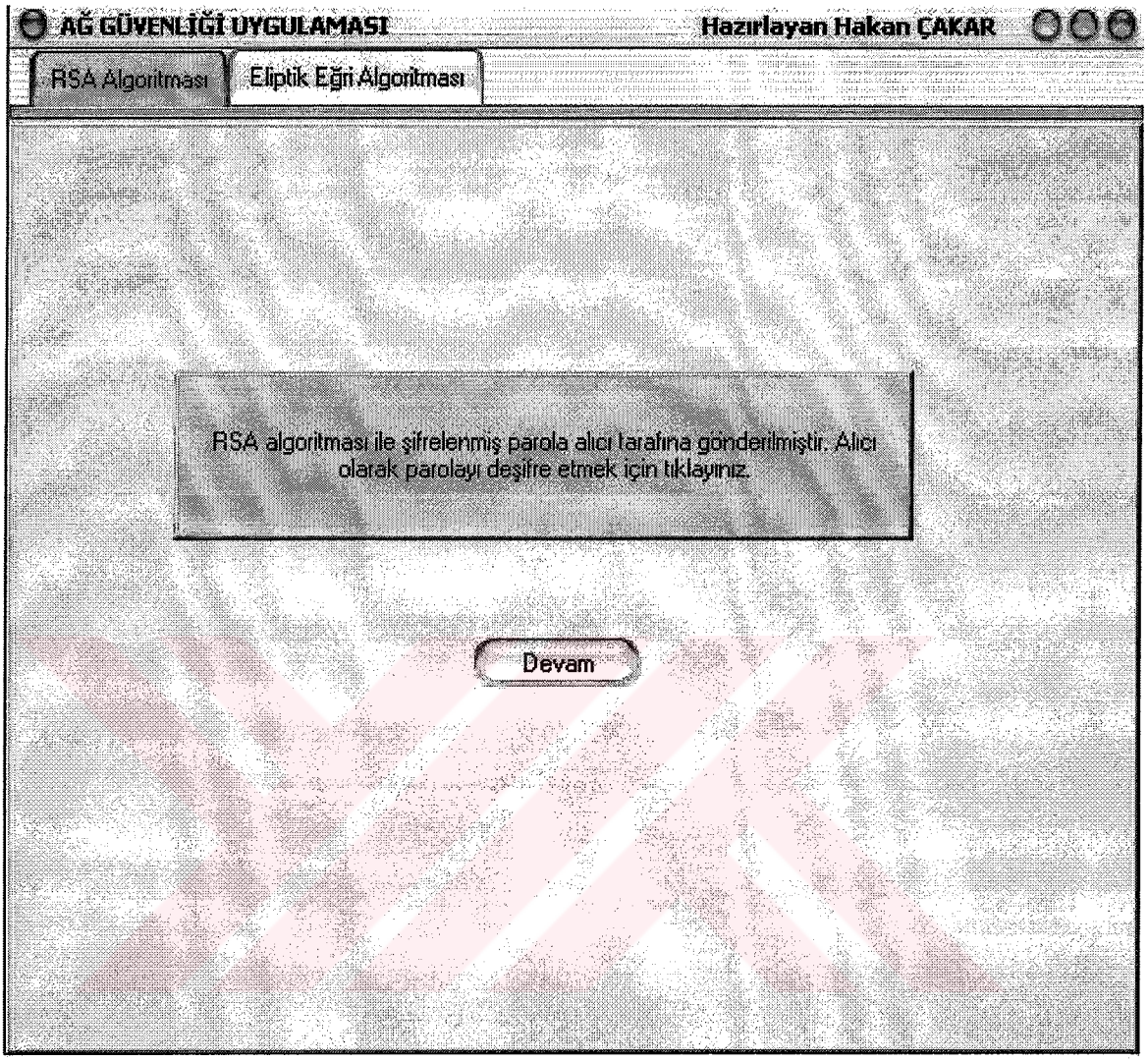
Şekil 7.3. Şifrelenecek Parolanın Girilmesi

Şekil 7.3. 'de şifrelenecek olan M parolasının girilmesi sağlanmaktadır. Girilecek olan parolanın 4 haneli olmasında fayda vardır. Uygun parola girildikten sonra, **RSA şifreleme** butonuna tıklanır. Program, ekran görüntüsünde verilmiş olan şifreleme formülüne göre hesaplanan sonucu, ikili sayı sistemine dönüştürmektedir.



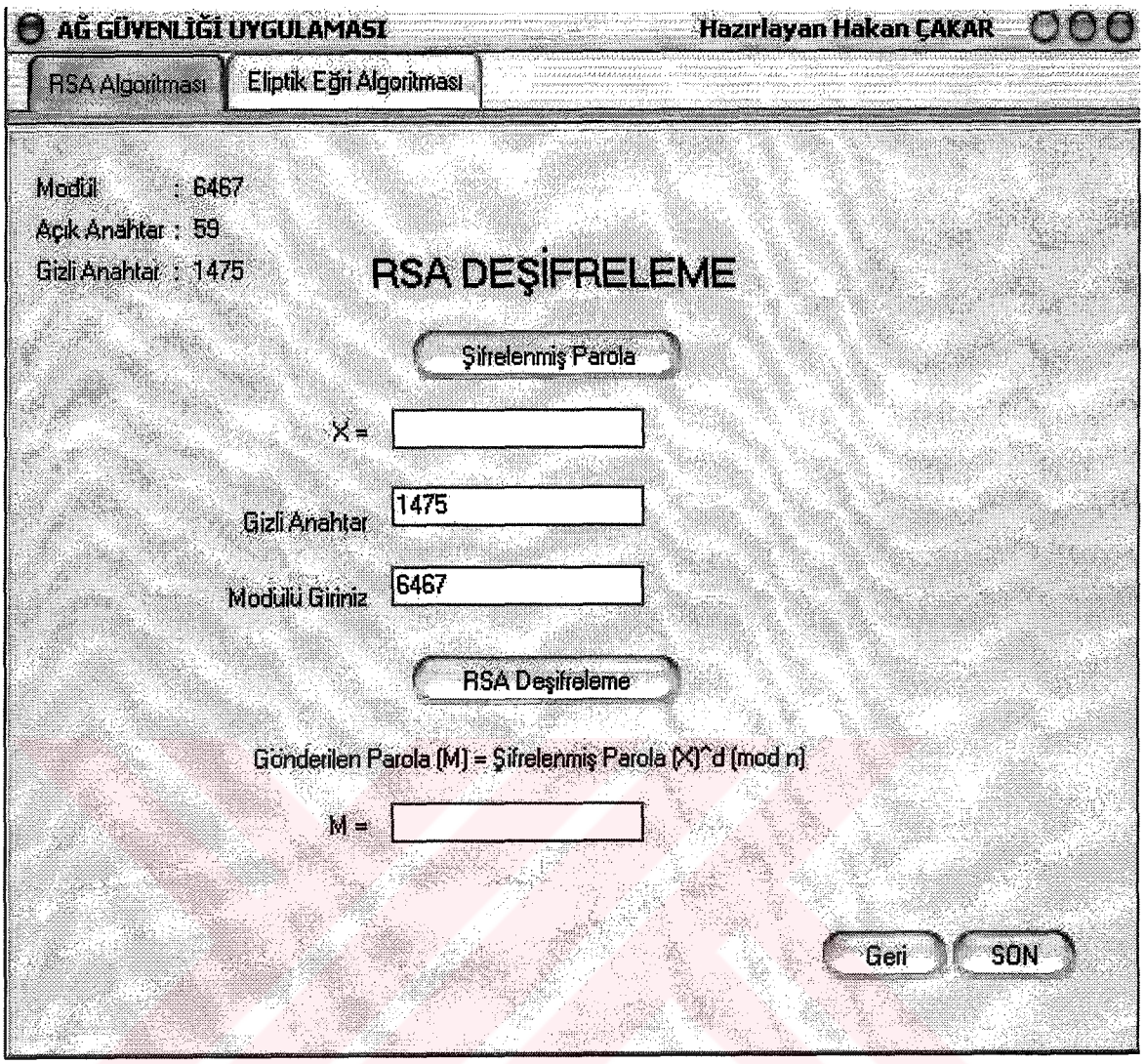
Şekil 7.4. Girilen Parolanın RSA Algoritması Kullanılarak Şifrelenmesi

Şekil 7.4.' de M parolası **0007** seçilmiştir. Modül, açık anahtar ve gizli anahtar da mevcut olduğundan **RSA şifreleme** butonuna tıklandıktan sonra, şifreli parola **001101111110** şekline dönüştürülmüştür. Bu aşamada **Geri** butonuna tıklanıp, bir önceki ekran görüntüsü elde edilebildiği gibi, **Parolayı Gönder** butonuyla da bir sonraki kısma geçilebilmektedir.



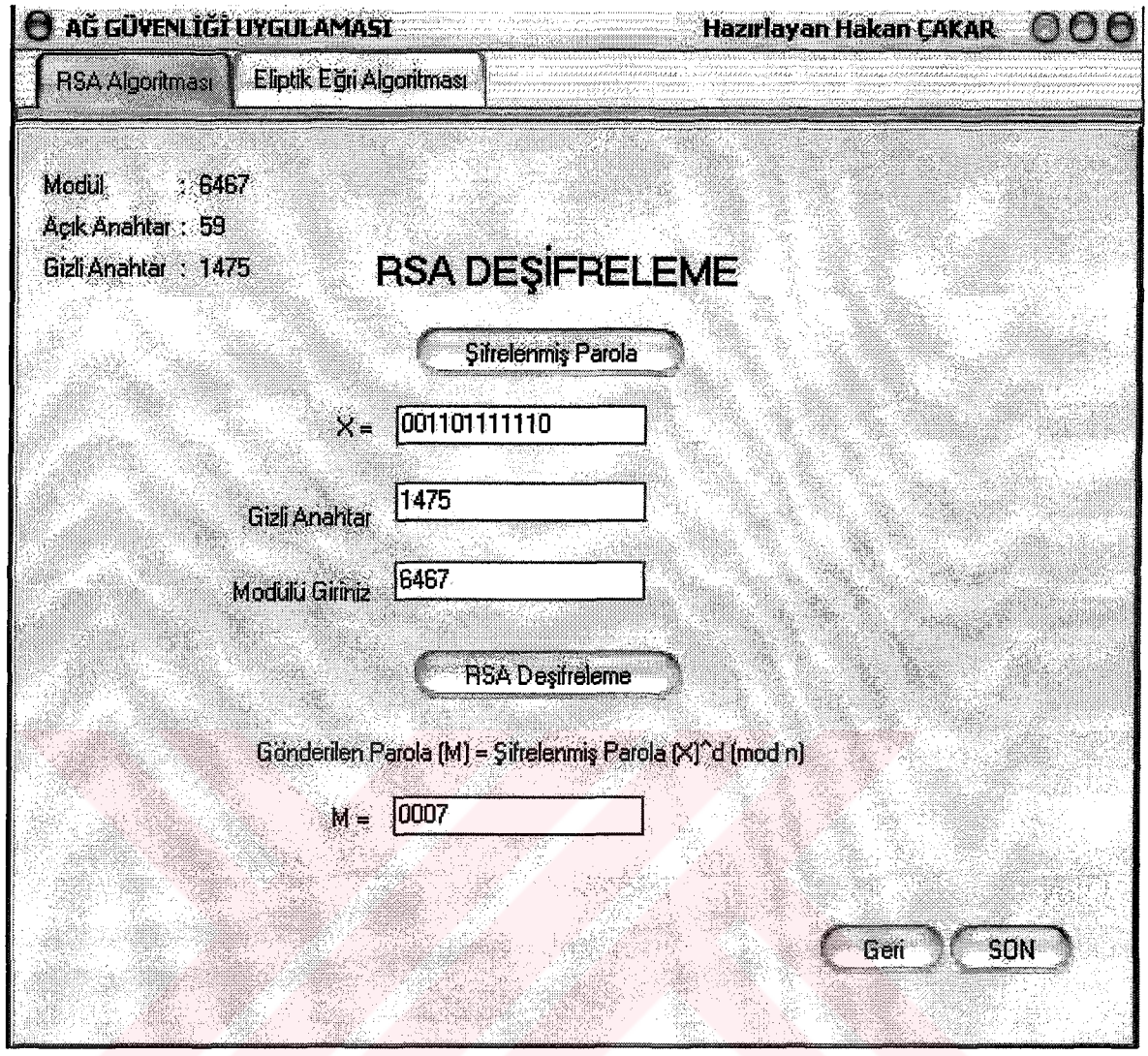
Şekil 7.5. Şifrelenmiş Parolanın Alıcı Tarafa Gönderilmesi

Şekil 7.5. ise, şifrelenmiş parolanın alıcı tarafta bulunan kullanıcıya gönderildiği mesajını veren ekran görüntüsüdür. Bu mesaj alındıktan sonra, **Devam** butonuna tıklanmalıdır.



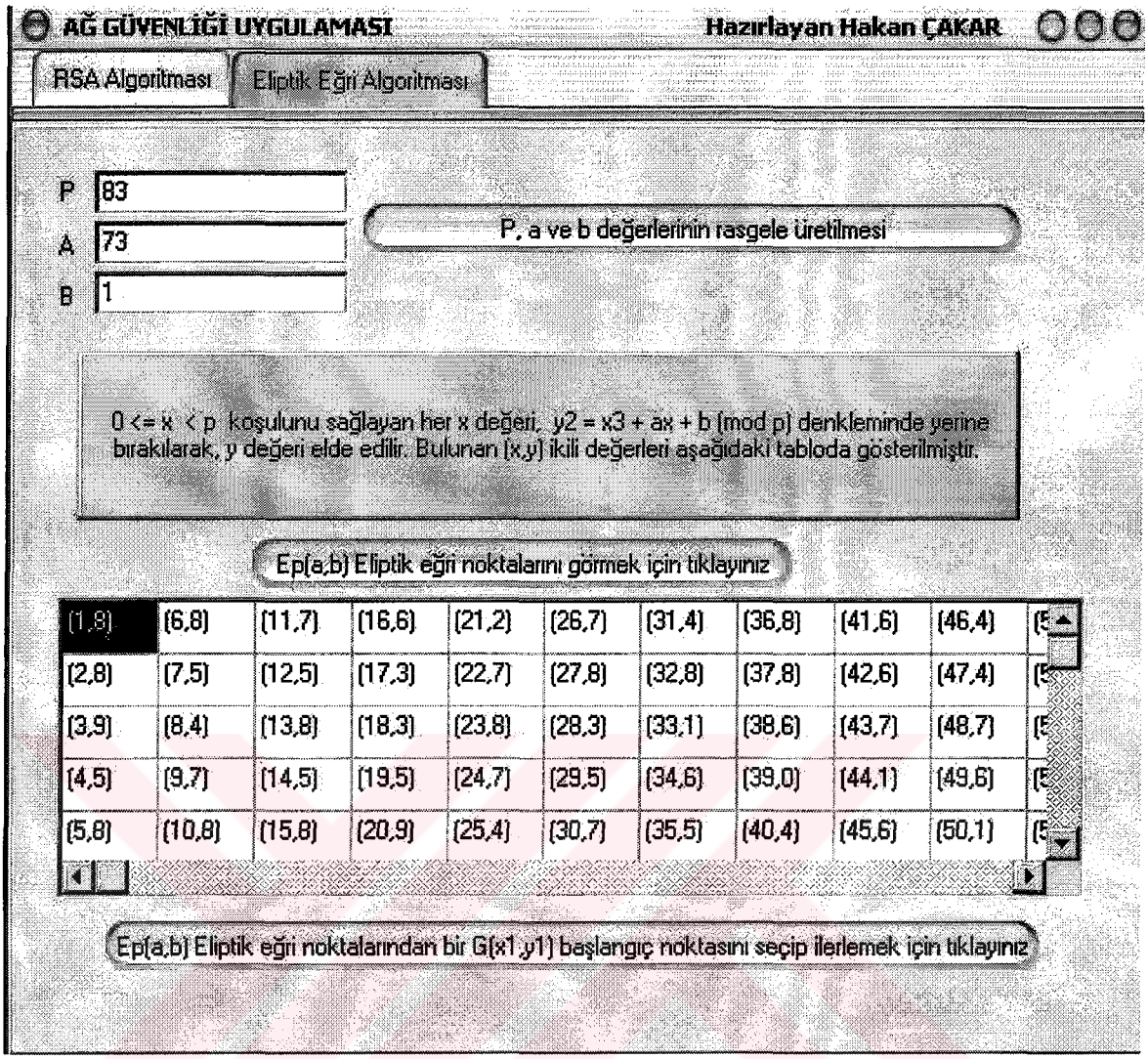
Şekil 7.6. Şifrelenmiş Parolanın Alıcı tarafından Görülmesi

Yukarıdaki şekilde, RSA deşifreleme aşamasının gerçekleştirildiği ekran görüntüsü verilmiştir. İkilik sistemde bulunan şifrelenmiş parolanın görülebilmesi için, **Şifrelenmiş Parola** butonuna tıklanmalıdır. Şekil 7.7' de, butonlara tıklandıktan sonra karşılaşılan sayısal değerler görülmektedir.



Şekil 7.7. Şifrelenmiş Parolanın RSA Algoritması Kullanılarak Deşifre Edilmesi

Şifrelenmiş parola butonuna tıklandığında, **001101111110** şeklindeki şifrelenmiş parola görülür, daha sonra **RSA Deşifreleme** butonuna tıklanır. Şekil 7.7' de verilen deşifreleme formülüne göre hesaplamalar yapıldığında, orijinal parola 0007 elde edilmektedir. Yine önceki şekillerde olduğu gibi **Geri** butonuyla bir önceki ekran görüntüsü görülebildiği gibi, **SON** butonuyla da işlemler sonlandırılmaktadır.

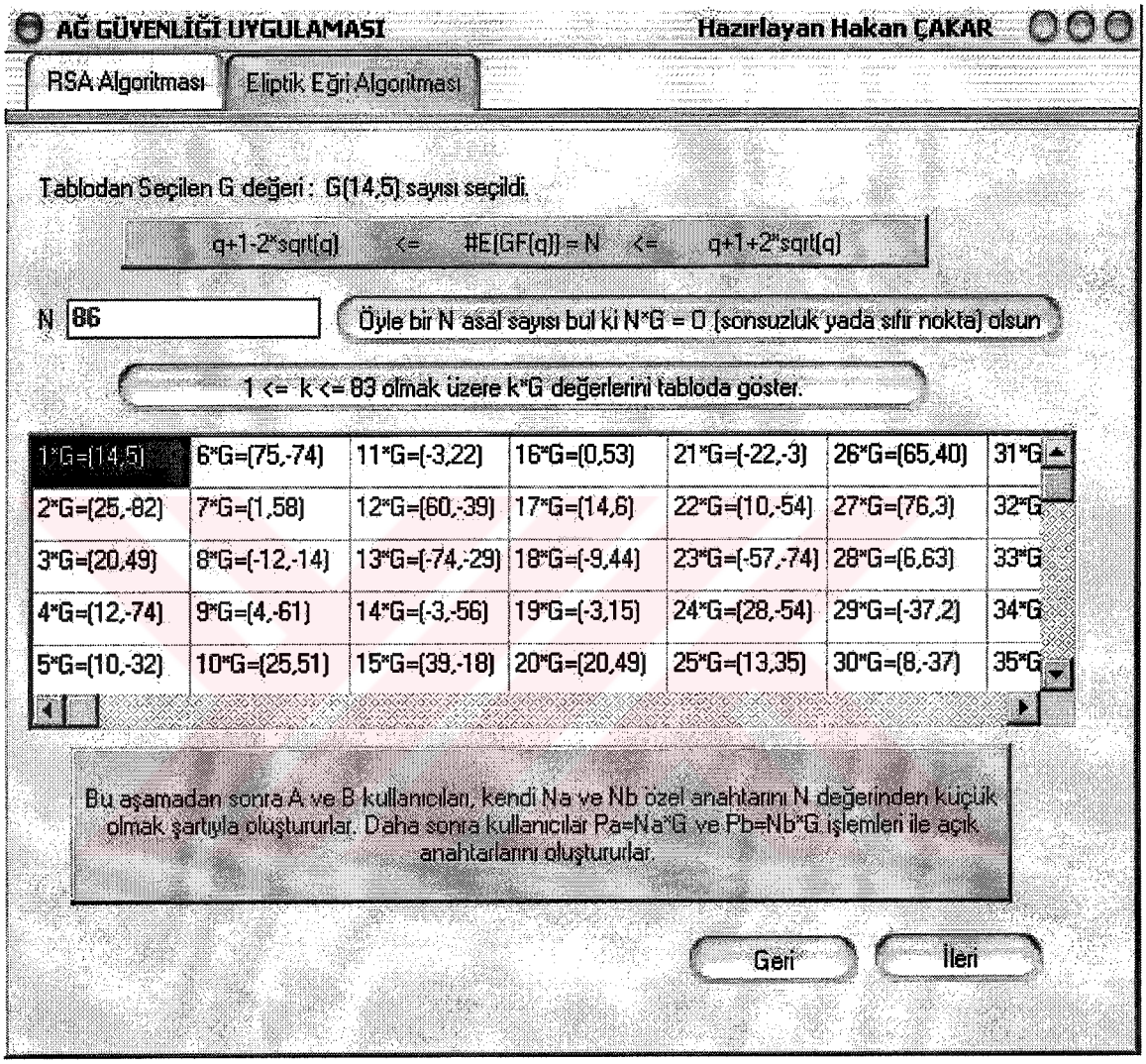


Şekil 7.8. Eliptik Eğri Noktalarının Oluşturulması

Bu kısım, program da Eliptik eğri algoritması formuna geçildiğinde ilk karşılaşılan arayüzdür. Burada modülo P, a ve b değerlerinin üretilmesi sağlanmaktadır. Bu değerlerin üretilmesi, asal sayı belirleme algoritmasına göre sağlanmaktadır.

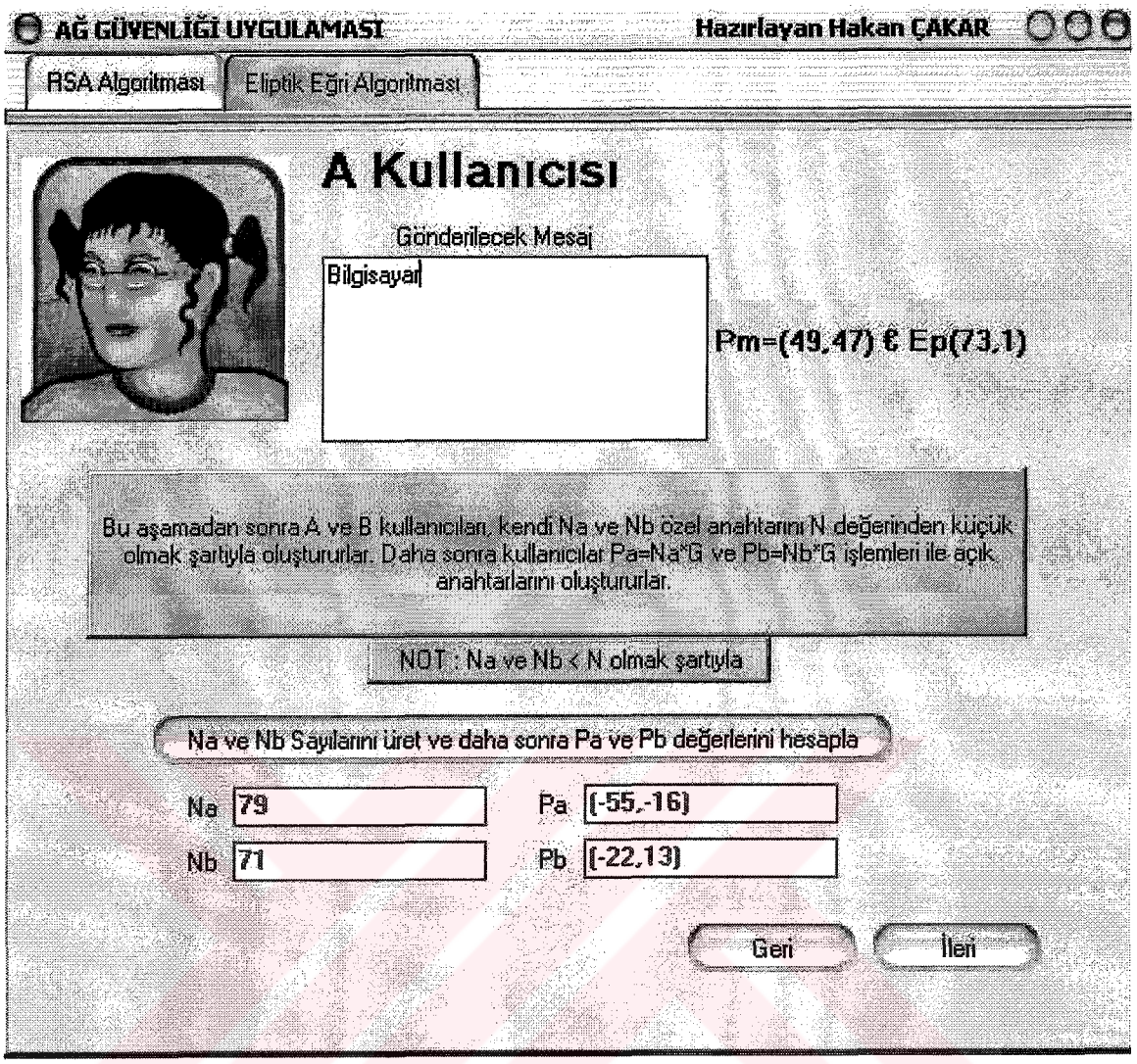
Elde edilen bu sayılar, $y^2 = x^3 + ax + b \pmod p$ denkleminde kullanılmaktadır. Şekil 7.8' de verilen açıklamaya uygun bulunan (x,y) ikili değerlerinin tablo olarak gösterilmesi de yine bu kısımda yapılmaktadır. Şekil üzerinde bulunan en alttaki butonun kullanılma amacı ise, Eliptik eğri nokta gurupları arasından G(x1,y1) gibi bir başlangıç noktası (generator point) elde etmek içindir.

Şekil 7.8' de, rasgele seçilen P, a ve b değerlerinin Eliptik eğri denkleminde kullanılması sonucunda elde edilen (x,y) şeklindeki Eliptik eğri noktaları görülmektedir. Bu noktalar arasından bir G başlangıç noktasının seçimi ve sonraki işlemler Şekil 7.9' da verilmiştir.



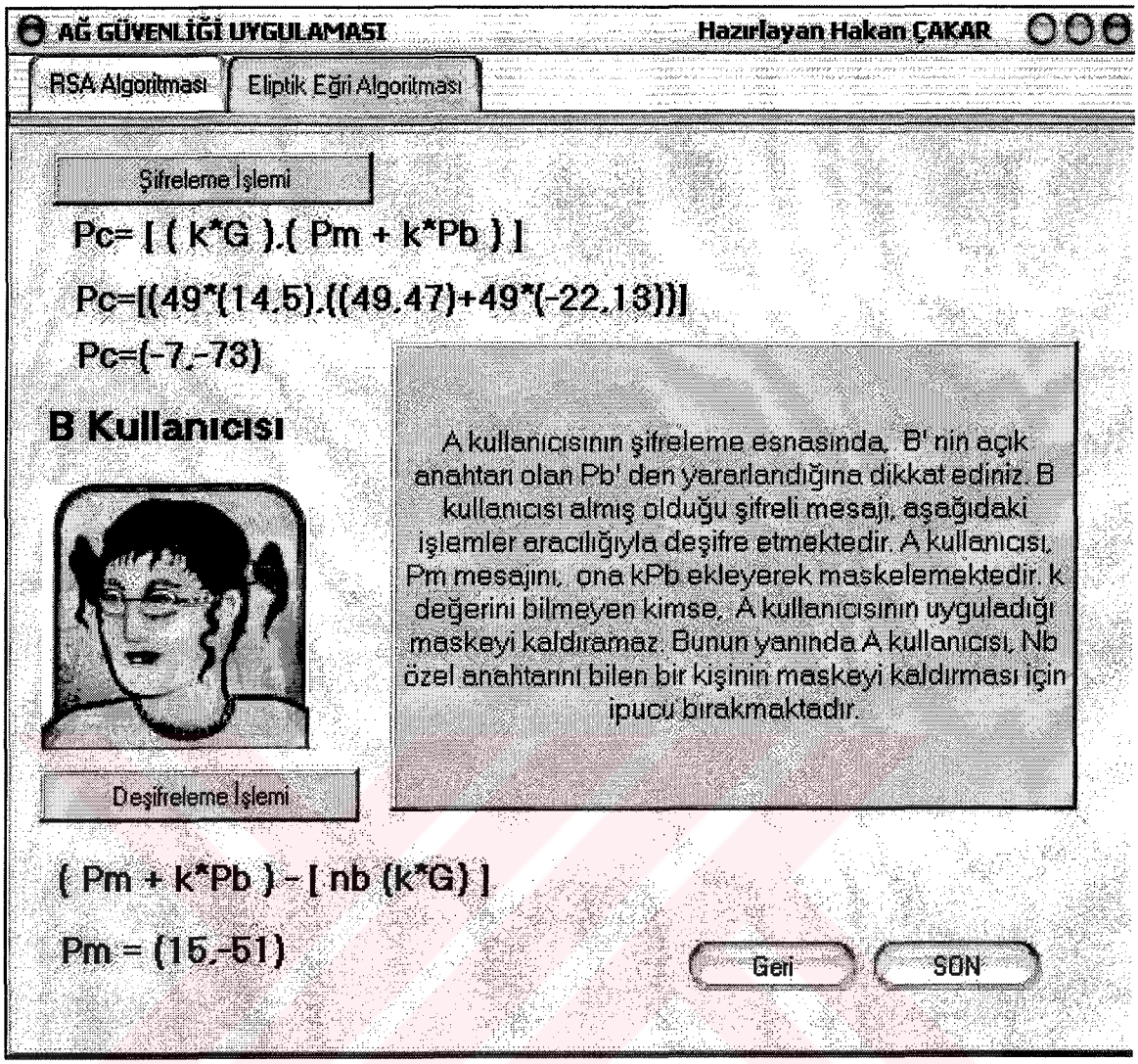
Şekil 7.9. G Başlangıç Noktasının Belirlenmesi ve k*G Değerlerinin Tablo Olarak Gösterilmesi

Şekil 7.9' da, tablodan seçilen G başlangıç noktası değerinin (14,5) olduğu görülmektedir. Daha sonra N*G = 0 (Sonsuzluk yada sıfır nokta) olacak şekilde, bir N asal sayısı seçilir, N sayısı burada 86 olarak belirlenmiştir. Tablonun üstünde bulunan butona tıklandığında, değerler liste şeklinde karşımıza çıkmaktadır. Bir sonraki aşamaya geçmek için **İleri** butonuna tıklanır.



Şekil 7.10. Gönderilecek Mesajın Girilmesi ve Anahtarların Belirlenmesi

A kullanıcısı bu aşamada gönderilecek mesajı girmekte ve bu belirlenen mesaj, P_m şeklinde eliptik eğri üzerinde bir noktaya karşılık getirilmektedir. Bu nokta aynı zamanda E_p' nin elemanı olmalıdır. E_p (a,b) değerleri Şekil 7.8' de gösterilmiştir. Daha sonra N_a ve N_b özel anahtarları rasgele üretilir, $P_a = N_a * G$ ve $P_b = N_b * G$ formüllerine göre A ve B kullanıcılarının genel anahtarları elde edilir. Bir sonraki adım için **İleri** butonuna tıklanır.



Şekil 7.11. Eliptik Eğri Algoritmasına Göre Şifreleme ve Deşifreleme İşlemleri

Şekil 7.11' de de görüldüğü gibi, bir önceki adımda elde edilen değerler, Eliptik eğri algoritmasının kullandığı şifreleme yapısına göre şifrelenir ve B kullanıcısına gönderilir. Şifrelenmiş metni alan B kullanıcısı da Eliptik eğri algoritmasınının kullandığı deşifreleme yapısına göre metni çözmeye çalışır. Orijinal metnin elde edilebilmesi için B kullanıcısı, kendi açık ve özel anahtarını kullanmaktadır.

SON butonuna tıklandığında ise programdan çıkılabilmektedir. Aynı zamanda **Geri** butonu kullanılarak da, bir önceki kısımda yapılan işlemler takip edilebilmektedir.

7.5. RSA ve Eliptik Eğri Algoritmasının Performans Karşılaştırması

Tablo 7.4.` te, eliptik eğri metodu ile RSA` daki tamsayının iki asal çarpanına generalized number field sieve yöntemi ile ayrılması esnasında gereken hesapsal efor karşılaştırılmıştır. Tablodan da anlaşılacağı üzere, RSA` nın sağladığı direnci ECC, çok daha düşük anahtar boyutları ile sağlamakadır. Bu yüzden ECC, düşük anahtar boyutu ile sağladığı yüksek güvenlik sayesinde RSA` ya karşı büyük bir hesapsal üstünlük sağlamaktadır.

Tablo 7.3. Eliptik Eğri ve RSA Algoritması Karşılaştırması [9]

Pollard Rho yöntemi kullanarak Eliptik Eğri Algoritması		Genelleştirilmiş Sieve yöntemi kullanarak çarpanlara ayırma	
Anahtar	MIPS Yılı	Anahtar	MIPS Yılı
150	$3.8*10^{10}$	512	$3*10^{4}$
205	$7.1*10^{18}$	768	$2*10^{8}$
234	$1.6*10^{28}$	1024	$3*10^{11}$
		1280	$1*10^{14}$
		1536	$3*10^{16}$
		2048	$3*10^{20}$

8. SONUÇLAR VE ÖNERİLER

8.1. Sonuçlar ve Tartışma

Bu tez çalışmasında, yaygın olarak kullanılan açık anahtarlamalı şifreleme yöntemlerinden olan RSA ve Eliptik Eğri algoritmaları kullanılarak bir metnin, şifreleme ve deşifreleme aşamaları adım adım gösterilmiş ve bu algoritmalar nesne tabanlı bir bilgisayar programlama dilinde uygulama haline dönüştürülmüştür. Temel amaç, ileride yapılabilecek donanım tabanlı uygulamalara zemin oluşturmaktır. Şifreleme işlemlerinde en çok kullanılan şifreleme algoritması RSA' dır. Bu algoritma günümüzde 160 bit sayısal anahtar büyüklükleri ile gerçekleştirilmektedir. Ancak gelecek için daha hızlı ve daha çok işlem yeteneğine sahip bilgisayarların ortaya çıkması bu anahtar büyüklüğünün yetersiz kalmasına sebep olacaktır. RSA algoritması ile Eliptik eğri algoritmasının karşılaştırılmasından da anlaşılacağı gibi gelecekte kullanılması gereken 1024 bit uzunluğundaki eliptik eğri anahtarları aynı işlemleri daha kısa sürede gerçekleştirebildiği gibi, daha düşük anahtar boyutu sağlamasından dolayı gerekli hafıza miktarını da azaltmaktadır. Bu da gösteriyor ki Eliptik Eğri algoritması gerek hız, gerek anahtar uzunluğu, gerekse süre gibi etkenlerden dolayı en çok kullanılması gereken algoritma olmalıdır.

8.2. Öneriler

Bu tezin en önemli bölümü, kuşkusuz RSA ve Eliptik Eğri algoritmalarının uygulamasının gerçekleştirildiği kısımdır. Bu tür bir çalışmanın yapılabilmesi için ileri derecede matematik bilgisi gerekmektedir. Ayrıca en önemlisi ise uygun bir yazılım geliştirmekteki yaşanan zorluklardır.

Bu tez kapsamında şifreleme ve deşifreleme işlemeleri için kullanışlı bir yazılım geliştirilmiş olmakla birlikte, bu konuda daha kapsamlı çalışmaların yapılması önerilmektedir.

9. KAYNAKLAR

[1] Varol, A., Alkan, T., 1998, İnternet'e Genel Bakış, Uzaktan Eğitim, 10-16

[2] Varol, A., 2001, İnternet Ortamında Oluşabilecek Yeni Suç İşleme Yöntemleri ve Çözüm Önerileri, BTIE 2001, Bilişim Teknolojileri Işığında Eğitim Konferansı ve Sergisi, 313-319

[3] Taşdemir, M., 2001, Ağ Güvenliği için PC Tabanlı bir Paket Filtreleme Sisteminin Tasarımı ve Gerçekleştirimi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

[4] TCP/IP Protokolü, http:// www.bilgisayarogren.com/network7.doc

[5] Postel, J. (ed.), 1981, RFC 791, Internet Protocol, DARPA Internet Program Protocol Specification, USC/Information Sciences Institute

[6] Kodaz H., 2003, RSA Şifreleme Algoritmasının Uygulaması, Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Alaeddin Keykubad Kampusü

[7] Windows 2000 Advanced Server, ISA Server 2000, http://www.microsoft.com.tr

[8] ISA Server, http://www.farukcubukcu.com

[9] Açık Anahtarlı Kriptografi (Eliptik Eğri Kriptografisi), http://www.enderunix.org/doc/pkc.html

ÖZGEÇMİŞ

Hakan ÇAKAR
hcakar@firat.edu.tr
Tlf: 424 2370000 / 6656
Fırat Üniversitesi Teknik Eğitim Fakültesi
Elektronik Bilgisayar Eğitimi Bölümü
ELAZIĞ

1980 yılında Elazığ'da doğdu. İlk, orta ve lise öğrenimini Elazığ'da tamamladıktan sonra 1997 yılında Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nü kazandı. 2001 yılında bu bölümden mezun oldu. 2002 yılında Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektronik Bilgisayar Eğitimi Ana Bilim Dalı Bilgisayar Sistemleri Bilim Dalı'nda yüksek lisans eğitimine başladı. 2001 yılı Kasım ayında Fırat Üniversitesi Rektörlüğü Enformatik Bölümü tarafından yapılan Okutmanlık sınavını kazanarak 2001 yılı Aralık ayında bu göreve başladı. Halen bu görevi Fırat Üniversitesi Teknik Eğitim Fakültesi Elektronik-Bilgisayar Eğitimi bölümünde sürdürmektedir. Yabancı dili ingilizcedir.