T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

RSA ŞİFRELEME YÖNTEMİ ve ÖZELLİKLERİ ÜZERİNE

Hazırlayan
Sümeyye ENGİN

Danışman
Dr. Öğr. Üyesi Emin AYGÜN

Yüksek Lisans Tezi

Eylül 2020
KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

RSA ŞİFRELEME YÖNTEMİ ve ÖZELLİKLERİ ÜZERİNE

(Yüksek Lisans Tezi)

Hazırlayan
Sümeyye ENGİN

Danışman
Dr. Öğr. Üyesi Emin AYGÜN

Eylül 2020
KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Sümeyye ENGİN

YÖNERGEYE UYGUNLUK

"Rsa Şifreleme Yöntemi ve Özellikleri Üzerine" adlı Yüksek Lisans Tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi' ne uygun olarak hazırlanmıştır.

Hazırlayan
Sümeyye ENGİN

Danışman
Dr. Öğr. Üyesi Emin AYGÜN

Matematik ABD Başkanı

Prof. Dr. Hüseyin ALTINDİŞ

Dr. Öğr. Üyesi Emin AYGÜN danışmanlığında **Sümeyye ENGİN** tarafından hazırlanan **"Rsa Şifreleme Yöntemi ve Özellikleri Üzerine"** adlı bu çalışma jürimiz tarafından Erciyes Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

/ / 2020

JÜRİ:

Danışman : Dr. Öğr. Üyesi Emin AYGÜN
Üye : Prof. Dr. Muammer KULA
Üye : Dr. Öğretim Üyesi Bahatdin DAŞBAŞI

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulunun ……...… tarih ve ……..……sayılı kararı ile onaylanmıştır.

……. /……../ ……

Prof. Dr. Mehmet AKKURT

Enstitü Müdürü

TEŞEKKÜR

Bana çalışmalarım süresince her türlü yardımı ve fedakârlığı sağlayan, yoğun çalışma şartlarına rağmen emeğini hiçbir zaman esirgemeyen sayın danışman hocam Dr. Öğr. Üyesi Emin AYGÜN ’e, kitabından son derece istifade ettiğim kıymetli hocam Prof. Dr. Hüseyin ALTINDİŞ’ e ve tez yazım aşaması boyunca desteklerini hep hissettiğim eşim ve aileme sonsuz teşekkürlerimi sunarım.

Sümeyye ENGİN

Eylül 2020, KAYSERİ

RSA ŞİFRELEME YÖNTEMİ VE ÖZELLİKLERİ ÜZERİNE

Sümeyye ENGİN

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Eylül 2020
Danışman: Dr. Öğr. Üyesi Emin AYGÜN

ÖZET

Geçmişten günümüze kadar geçen zamanda bilgi, ülkeler arası savaşta önemli unsurlardan bir tanesi olmuştur. Bununla birlikte bilginin saklanması, korunarak alıcısına iletilmesi önem kazanmıştır. Metnin şifrelenerek karşı tarafa ulaştırılması sırasında oluşabilecek saldırılara karşı daha güvenli algoritmalar oluşturulmuştur. Temeli çarpanlara ayırma zorluğuna dayanan RSA Şifreleme Algoritması, bunlardan bir tanesidir. 1978' de Ron Rivest, Adi Shamir ve Lon Adleman tarafından öne sürülen bu algoritma, bilginin istenen koşullarda saklanması ya da alıcısına iletilmesinin sağlanması için tercih edilen en ön plandaki algoritmalardan biridir. Şifreleme yapmak için kullanılacak anahtarı oluşturmak için seçilen iki asal sayının büyüklüğü, bu şifreleme metodunun güvenilirliğini artıracaktır. Yalnız güvenilirliği ne kadar artırsak da gelişen teknoloji ve bilgisayar sistemleri sebebiyle bu kriptolojik yapı bir takım saldırılara maruz kalacaktır. Alıcısına ulaşmadan üçüncü kişiler tarafından orijinal metni ele geçirmeye yönelik yapılan bu saldırılar da şifreyi kırma oldukça zaman alacaktır. Bu nedenle de alıcısı tarafından deşifrelenmesi uzun sürmesine rağmen günümüz de hala tercih edilmektedir.

Anahtar Kelimeler: Kriptoloji, RSA Şifreleme Algoritması, RSA'ya karşı yapılan saldırılar.

ON RSA ENCRYPTION METHOD AND PROPERTİES

Sümeyye ENGİN

Erciyes University, Graduate School of Natural and Applied Sciences

Master Thesis, September 2020

Supervisor: Dr. Öğr. Ü. Emin AYGÜN

ABSTRACT

Information has been one of the important elements in the war between countries from the past to the present. However, it has gained importance to keep the information and to transmit to its recipient. Safer algorithms have been created against attacks that may occur during the encryption of the text and delivery to the other party. The RSA Encryption Algorithm, which is based on the difficulty of factoring the foundation, is one of them. This algorithm, proposed by Ron Rivest, Adi Shamir and Lon Adleman in 1978, is one of the most preferred algorithms to ensure that information is stored or transmitted to its recipient. The size of the two prime numbers chosen to generate the key to be used for encryption will increase the reliability of this encryption method. However, no matter how much we increase reliability, this cryptological structure will be exposed to some attacks due to the developing technology and computer systems. These attacks, which are carried out by third parties before they reach their recipients, to take the original text will also take a long time to crack the password. Therefore, although it takes a long time to decipher it by its receiver, it is still preferred today.

Keywords: Cryptology, RSA Encryption Algorithm, Attacks against RSA

İÇİNDEKİLER

RSA ŞİFRELEME YÖNTEMİ VE ÖZELLİKLERİ ÜZERİNE

Sayfa

2. BÖLÜM

GENEL ŞİFRELEME ALGORİTMALARI

3. BÖLÜM

RSA ŞİFRELEME ALGORİTMASI

KISALTMALAR

Sembol	Anlamı
$\boldsymbol{M}$	Açık Metin (Mesaj)
$\boldsymbol{C}$	Kapalı Metin
$\boldsymbol{E}$	Şifreleme İşlemi
$\boldsymbol{D}$	Deşifreleme İşlemi
$\boldsymbol{m}$	Düz metin, şifrelenmemiş metin, şifrelenmemiş mesaj
$\boldsymbol{c}$	Şifrelenmiş metin, şifreli metin, şifreli mesaj
NIST	National Institute of Standards and Technology
DES	Veri Şifreleme Standardı
FBI	Federal Bureau of Investigation
IDEA	Uluslararası Veri Şifreleme Algoritması
PKI	Açık Anahtar Altyapısı
RSA	Rivest-Shamir-Adleman
NSA	ABD Ulusal Güvenlik Kurumu
FIPS	Federal Bilgi İşlem Standardı
ECC	Eliptik Eğri Kriptografisi
PGP	Pretty Good Privacy
SHA	Güvenli Özetleme Algoritması
ABD	Amerika Birleşik Devletleri
AES	Gelişmiş Şifreleme Standardı
3DES	Üçlü Veri Şifreleme Standardı
MD5	Mesaj Özetleme Algoritması 5
SSL	Soket Düzeyi Güvenlik

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GİRİŞ

Yazının icadını insanlık tarihinin başlangıcı olarak kabul edersek, yazıyla birlikte bilgi toplanabilir, saklanabilir ve başka kişi ve birimlere iletilebilir hale gelmiştir. İşte yazının icadından günümüze kadar olan bu sürede insanlar, iletişimde bilgi gizliliğini hep ön planda tutmuşlardır. Çünkü ünlü düşünür Francis Bacon'un da yüzyıllar önce ifade ettiği gibi bilgi, bir güçtür. Bu nedenle toplumlar, birbirlerine üstünlük sağlayabilmek için ağır ve mekanik silahları kullanmak yerine 1990'lı yılların başlarında yeni bir kavram olarak dünya literatürüne giren, maddi ve manevi açıdan daha az kayıpla sonuçlanabilen sessiz savaşı yani Bilgi Savaşı'nı kullanmaya başlamıştır. Bilginin güvenli şekilde saklanıp korunması ve sürekli olarak güncellenmesi toplumların üstünlüklerinin ya da özgürlüklerinin devamı anlamına geldiği için bilginin iyi korunması, toplumların hayatta kalması için en önemli unsur haline gelmiştir. Geçmişten günümüze kadar geçen sürede çeşitli kültürler, bilgi güvenliğini sağlayabilmek için değişik yöntemler geliştirmiş ve uygulamışlardır. Bilginin korunumu ve güvenli haberleşme, bilginin şifrelenmesi, değiştirilerek karşı tarafa güvenli bir şekilde aktarılması ihtiyacı sonucunda geliştirilen bu yöntemler ise kriptoloji biliminin var olmasını ve gelişmesini sağlamışlardır [3, 6, 13, 14, 20, 26, 29].

Gelişen kriptoloji bilimiyle birlikte şifreleme algoritmaları çeşitlenmiş, içlerinden anahtarlı şifreleme yöntemine örnek olan RSA Şifreleme Metod'u diğerlerine göre daha fazla önem kazanmıştır. Çünkü geliştirilen anahtarların boyutunun uzun tutulmasıyla güvenilirliği yüksek bir yöntem olmuş ve bu sebeple de günümüzde bile hala tercih edilebilen bir şifreleme sistemi haline gelmiştir. İşte biz bu tezde en genel hatlarıyla RSA Şifreleme Sistemi'ni inceleyeceğiz.

Tezin birinci bölümünde kriptolojiye giriş yapıp tanımını verdikten sonra tarihi hakkında genel bir bilgi vereceğiz. Kriptogarafi ve kriptoanaliz kavramlarından bahsedip 'Kriptolojinin amacı nedir?', 'Kriptolojinin kullanım alanları nelerdir?' bunlara değineceğiz. Ayrıca temel matematiksel kavramları vereceğiz.

Tezin ikinci bölümünde genel şifreleme algoritmalarını inceleyeceğiz. Kullanıldığı anahtarın türüne göre çeşitlenen simetrik şifreleme ve asimetrik şifreleme algoritmalarını anlatacağız. İki şifreleme algoritmasının karşılaştırmasını yaptıktan sonra elektronik ortamda şifrelemede önemi olan sayısal imza ve sayısal sertifika konularını açıklayacağız. Son olarak hybrit şifrelemeye değinerek bu bölümü sonlandıracağız.

Tezin üçüncü bölümünde ana konumuz olan RSA Şifreleme Yöntemi'ne giriş yapacağız. En genel özellikleriyle bu yöntemi anlatılıp tarihinden bahsedeceğiz. RSA' nın genel yapısı, anahtar oluşumu, şifreleme ve deşifreleme işlemlerini anlatacağız. Yeteri kadar örnekleme yaptıktan sonra bu yöntemin hızını artıran unsurlardan bahsedeceğiz. Son olarak ta sayısal imzayı RSA Yöntemi'ne uygulayarak gerçekleştirmeyi açıklayacağız.

Tezin dördüncü bölümünde ise RSA'nın kriptoanalizi yapılacak ve bu yönteme karşı yapılabilecek olan saldırıları anlatacağız. RSA şifreleme metodunun diğer benzer metotlarla karşılaştırılması yapılarak bu bölüme son vereceğiz.

1.BÖLÜM
KRİPTOLOJİ

1.1. Kriptolojinin Tanımı

Şifreleme bilimi olan kriptoloji, haberleşmede veri güvenliğini sağlayan kriptocihazlarını, bu cihazlarda kullanılan algoritmaların güvenilirliğini araştıran, matematik bazlı bir bilim dalıdır. En temel ifade şekliyle, bilginin başkaları tarafından okunamayacak formlara çevrilmesi ve özel teknikler kullanarak sadece ilgili kişiler vasıtasıyla eski haline dönüştürülme işlemidir [18]. Kriptolojide amaç, üçüncü kişilerin bir takım saldırılarla orijinal metne ulaşmasını engelleyecek şekilde iletilecek metin ya da mesajın şifrelenmesidir. Böylece şifrelenen mesaj başkaları tarafından ele geçirilse bile deşifrelemek için gerekli olan bilgilere sahip olmadıkları için mesajı kırmaları mümkün olmayacaktır. Bu da bilginin güvenliği bir noktaya kadar sağlanmış ve de şifreleme işleminin yaygınlaşmasına olanak sağlamış demektir [25].

Herkes tarafından okunabilen metinlerin orijinal bir başka deyişle şifrelenmemiş hali olan ve kriptolojinin özü plaintextte denilen düz metnin içeriğini başka kişiler tarafından öğrenilmesini önleyip saklamak için yapılan işlem, şifreleme işlemidir. İletinin üçüncü şahıslar tarafından ele geçirilmesini önlemek için oluşturulan yeni metin ise şifreli metindir. Oluşturulan bu şifreli metni düz metne çevirme işlemi ise deşifreleme bir başka deyişle şifre çözme işlemi olarak ifade edilir ve sadece alıcıda bulunan bilgiler vasıtasıyla gerçekleştirilir [23].

1.2. Kriptolojinin Amacı

Verinin şifrelenme amacı ya bilgiyi güvenli bir şekilde saklamak ya da güvenli bir şekilde ulaşılması istenen kişiye gerekli mesajı iletmektir. Düz metni şifreleyebilmek ve şifrelenmiş metni çözebilmek için kullanılan algoritma parçasına anahtar denir.

Şifrelenmiş bilgi ya da mesajın güvenilirliği ise algoritmanın güçlüğüne ve bahsi geçen anahtarın gizliliğine bağlıdır.

Şekil 1. 1. Şifrelemenin ana şeması

Yunanca saklanmış, gizli anlamına gelen kriptos ve söz, bilgi, bilim gibi birçok anlamı olan logos kelimelerinden türetilmiş olan kriptoloji, kriptografi ve kriptoanaliz olmak üzere iki alt bilimden oluşur [1, 3, 5, 6].

Şekil 1. 2. Kriptolojinin bileşenleri

1.3. Kriptolojinin Kullanım Alanları

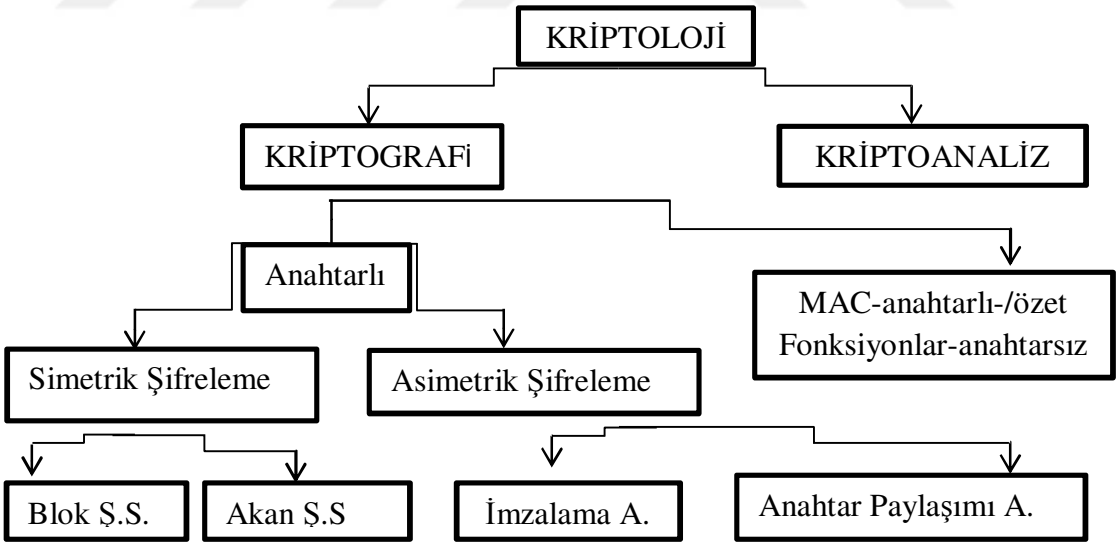
Askeri ve diplomasi haberleşmelerinde ön planda tutulan gizli haberleşme başka bir deyişle şifreleme, yaklaşık 4000 yıl önce kullanılmaya başlanmıştır [2, 23]. Şifreleme sistemini askeri iletişimde ilk uygulayan Spartalılardır. Geliştirdikleri cihazla askeri birlikler arasındaki haberleşmede gizli iletişimi sağlıyordu.

Şekil 1. 3. Spartalılar tarafından geliştirilen şifreleme cihazı [1]

Amacı gizlilik, veri bütünlüğü, doğrulama kimlik saptama ve inkâr edememe olan kriptoloji, insanlığın varoluşundan bu yana çeşitli evreler geçirerek günümüze gelmiştir [20]. Kriptoloji ilk olarak devletlerin ya da orduların kullandıkları gereç olsa da günümüzde herkesin hayatına girmiştir. 1990 tarihinden bu yana meydana gelen ve

gelişimsel olarak büyük bir hız kazanan teknoloji, gelişen teknolojiyle birlikte bilgisayar ve internetin insan hayatının her noktasında kullanılmaya başlanması kriptoloji biliminin önemini giderek arttırmıştır [1, 5].

Gelişen teknoloji ve bilgisayar sistemleri, bilginin korunmasını daha da gerekli kılmıştır. Çünkü gelişen her yenilik, bilginin başka kişilerin eline geçme ihtimalini artırmıştır. Özelliklede internet ortamında karşı tarafa ulaştırılması istenen bilginin, ağı dinleyenler tarafından bir takım saldırılara karşı açık olma ihtimalini doğurmuştur. Bilginin alıcısına ulaşmadan ele geçirilmesi, göndericinin kimliğinin tespit edilip ya da göndericiyi ve bilgisini olduğundan farklı göstererek alıcıyı yanıltmaya yönelik tehlikelere maruz kaldığından ağ ortamında da bilgi güvenliği hızla önem kazanmıştır. Bu güveni sağlayabilmekte şifrelenen metnin veya mesajın doğru bir şekilde iletilmesi ve metnin göndericisinden alıcısına iletildiği süre zarfı boyunca üçüncü kişiler tarafından dinlenmesini, şifrenin kırılıp düz metnin ele geçirilmesini önleme gereksinimlerini ortaya çıkarmıştır. Oluşan bu gereksinimler neticesinde iletişim sırasında anahtarlama yöntemine gidilmiştir [12]. Tablonun en genel hali:



Şekil 1. 4. En genel haliyle kriptolojinin yapısı [18]

1.4. Kriptogarafi

Kriptografi, alıcısına iletilmek üzere belirlenen metni şifrelemek ve şifrelenmiş metni de alıcısı tarafından orijinal hale getirmek yani şifreyi çözüp düz metni bulmak için

başvurulan metotların tamamını ifade eder [1, 20]. Amacı iletilmek veya saklanmak istenen bilginin, ulaşacağı kişinin deşifre edebileceği şekilde korunmasını sağlamak ve alıcısına iletmek olan bu teknoloji şifreleme ve deşifreleme işlemini gerçekleştirmek için kullanılan bir fonksiyondur. Bir başka deyişle şifrelenmek üzere bekleyen mevcut veriyi, alıcısı ve göndericisinden başka kişiler tarafından ele geçirilip okunamayacağı formata getirmek için uygulanan matematiksel algoritmalar bütünüdür [23]. Elektronik seçim, elektronik imza gibi alanlarda kullanıma açık olan kriptografinin amacı sadece mevcut metnin güvenli bir şekilde saklanması ve iletilmesine yönelik yöntemler oluşturmak değildir. Yunanca 'kryptos' ve 'graphein' kelimelerinin türetilmesiyle oluşan Kriptografi kimlik denetimi, bütünlük, gizlilik ilkelerini sağlamaya yönelik yapılan matematiksel işlemleri kapsar [3, 4, 26].

1.5. Kriptografik Algoritmalar

Kriptogarafide mantık, şifrelenmek istenen metnin matematiksel yöntemlerden faydalanılarak kodlanmasıdır. Bu matematiksel kodlama, kripto algoritması olarak ifade edilir. Başka bir deyişle Bir metni şifreleyebilmek ve şifrelenmiş metni deşifre edebilmek için uygulanan matematiksel işlemlerin tümüne Kriptografik Algoritmalar denir [19]. Bu algoritmanın gerçekleşmesi için şifrelenerek iletilmek ya da saklanmak istenen bir bilgi ve bu bilgiyi şifrelemeye uygun bir anahtar oluşturulmalıdır. Kriptogarafik sistemler, klasik ve modern olmak üzere iki alt grupta incelenir [21].

Şekil 1. 5. Yapısal olarak ikiye ayrılan kriptografik sistemler

Kullanılan anahtarın cinsine göre de asimetrik kriptografik sistemler ve simetrik kriptogarfik sistemler olmak üzere ikiye ayrılırlar. Burada bahsi geçen anahtarlar açık ve gizli anahtarlardır.

Göndericinin herkese yayınladığı, herkesin rahatlıkla ulaşabileceği anahtara açık anahtar denir.

Sadece alıcıda bulunan ve şifreli metni deşifrelemek için kullanılan anahtara gizli anahtar denir.

1.6. Kriptoanaliz

Kriptolojinin şifreleme bilimi ve alıcısına ulaştırılmak istenen metin ya da mesajın şifrelenerek iletilmesi amacı ile uygulandığından bahsetmiştik. Kriptanaliz de işte bu şifrelenen metinlerin çözülmesi bir başka deyişle orijinal metne ulaşılmak üzere analiz edilmesidir. Şifre çözme işlemi gerçekleştiren kişiye ise kriptoanalist denilmektedir [26]. Kriptografi metni veya mesajı şifreleyerek yazmak demekti. Kriptoanaliz ise bunun tam aksine şifre kırma, şifre çözme işlemidir. Kriptografi ile şifrelenen sistemin kriptoanaliz işlemi sayesinde kuvvetli ve zayıf olduğu noktaları tespit edilir. Yapılan bu tespitler de şifreleme yapmak için oluşturulan bütün anahtarları denemek için harcanacak süreyi ortadan kaldıracaktır. 9. yy da temeli frekans analizine dayalı ilk kayıtlı kriptoanaliz uygulaması Ebu Yusuf Yakup tarafından yapılmıştır. Yalnız 2. Dünya Savaş'ı sonrası şifreleme işlemleri yoğunlaşıp, bu sistemlerin daha karmaşık bir hal almasıyla birlikte kriptoanalizde matematik uygulamaları daha etkin olmaya başlamıştır. Özelliklede 1940 lı yıllarda 2. Dünya Savaş'ı sıralarında Nazilerin "Enigma" adını verdiği ve günümüzde güvenilirliği fazla olan algoritmalarda uygulanan, anahtar boyutuna sahip şifreleme makinesi kullanılmasına rağmen şifreli sistem bir takım ünlü kriptoanalistler tarafından çözülmüştür [1].

Şekil 1. 6. Enigma [1]

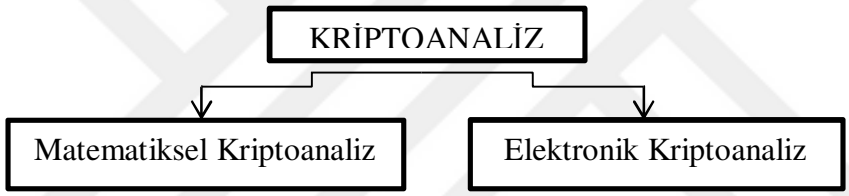
Bir takım kriptoanaliz yaklaşım tipleri vardır. Bunlar hedef odaklıdır ve odaklanan hedefe göre:

1. Matematiksel kriptoanaliz
2. Elektronik kriptoanaliz

olmak üzere iki kısma ayrılır.

Matematiksel kriptoanalizde algoritmada oluşan zayıf noktaları tespit edip bu noktalardan yapılan çıkarımlarla şifre çözme hedeflenir.

Elektronik kriptoanalizde ise algoritmada oluşan zayıf noktalardan değil de direk algoritma sisteminin çalışmasına yönelik olan şifre çözme işlemidir. Yani şifreleme sisteminin işleyici sırasında meydana gelen ayırt edici özelliklerden yola çıkarak kriptoanaliz gerçekleştirilir [14].



Şekil 1. 7. Odaklanan hedefe göre kriptoanaliz yöntemleri

1.7. Temel Matematiksel Kavramlar

Bu kısımda tezde bahsi geçen genel tanım ve teoremleri vermek için [6], [11], [12], [18] nolu kaynaklardan yararlanacağız.

Tanım 1.7.1: $a, b \in Z$ olmak üzere $a.c = b$ eşitliğini sağlayan bir $c \in Z$ varsa a böler b denir. Matematiksel olarak gösterim şekli ise $a|b$ dir.

Tanım 1.7.2: $a, b \in Z\ ve\ a \neq 0, b \neq 0$ olsun. Eğer $c > 0$ olmak üzere $c|a\ ve\ c|b$ ifadelerini sağlayan c tamsayısı mevcut ise bu 'c' tamsayısına a ile b tamsayılarının ortak böleni adı verilir.

Tanım 1.7.3: $ebob(a, b) = d$ şeklinde gösterilen ve

1. $d|a, d|b$

2. c tamsayı olmak üzere, bu c tamsayısı a ve b tamsayılarını bölüyor ise $c|d$ olduğunu söyleyebiliriz.

Özelliklerini sağlayan $d \in Z^+$ tamsayısına a ile b' nin en büyük ortak katı adı verilir.

Tanım 1.7.4: $p > 1\ ve\ p \in Z^+$ olmak üzere bu *p* pozitif tamsayısı *1* ve kendisinden başka bir sayıya bölünemiyorsa *p* asal sayıdır denir.

Tanım 1.7.5: $a, b \in Z$ olsun. Eğer *a* ve *b* nin *1* den başka ortak böleni yok ise bu iki sayıya aralarında asaldır denir.

Tanım 1.7.6: $a, b \in Z\ ve\ 0 < n$ olmak üzere *n* sayısı *a-b* ifadesini bölüyor ise *n* moduna göre *a* tamsayısı *b* tamsayısına denktir denir ve $a \equiv b(mod n)$ gösterimine sahiptir.

Tanım 1.7.7: *m* pozitif tamsayı olsun. *m* ile aralarında asal ve $0 \leq x \leq m - 1$ olacak şekilde ki *x* pozitif tamsayılarının sayısına *m*' nin Euler sayısı denir ve $\varphi(m)$ olarak ifade edilir.

Tanım 1.7.8: $a.x \equiv 1 mod(n)$ denkliği sağlansın. Bu denkliği sağlayan *x* sayısına *n* modülünde *a* sayısının aritmetik tersi denir.

Tanım 1.7.9: *a* sayısının *n* modülünde aritmetik tersi vardır ↔ *a* ile *n* aralarında asaldır.

Teorem 1.7.1: *p* asal sayı olmak üzere $\varphi(p) = p - 1$ dir diyebiliriz

Teorem 1.7.2: *p* ve *q* aralarında asal iki tamsayı olmak üzere $\varphi(p.q) = \varphi(p).(q)$ dir. Eğer *p* ve *q* asal sayılar ise $\varphi(p.q) = \varphi(p).(q) = (p-1)(q-1)$ olduğunu söyleyebiliriz.

Teorem 1.7.3: *a* ve *n* aralarında asal iki sayı olsun. O halde $a^{\varphi(n)} \equiv 1 mod(n)$ olduğunu söyleyebiliriz. Buna Euler Teoremi adı verilir.

Teorem 1.7.4: *p* sayısı *a* sayısını bölmeyen bir asal sayı olsun. O halde $a^{p-1} \equiv 1 mod(p)$ olduğunu söyleyebiliriz. Bu teoreme Fermat Teoremi adı verilir.

Teorem 1.7.5: $m_1, m_2, m_3, \ldots m_r \in Z^+$ olmak üzere bu sayılar ikişerli olarak aralarında asal olan sayılar olsun. $M = m_1, m_2, \ldots, m_r\ moduna\ göre\ x \equiv a_i mod(m_i), i = 1,2, \ldots., r$ sisteminin tek bir çözümü vardır. Bu teorem Çin Kalan Teoremi olarak ifade edilir.

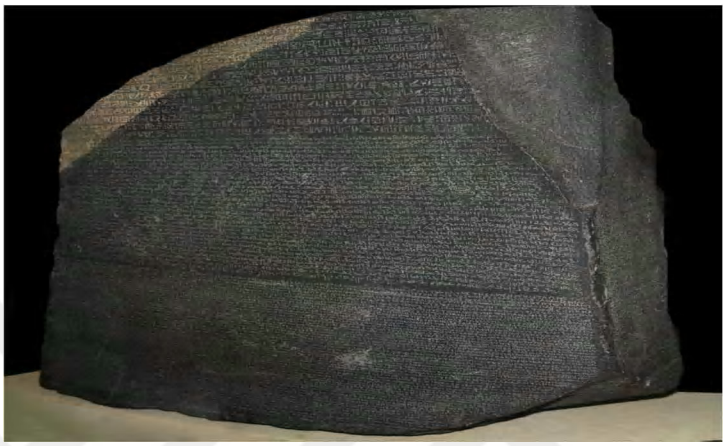
Teorem 1.7.6: $x \equiv a_i mod(m_i),\ i = 1,2, \ldots., r$ sisteminin bir çözümü vardır

↔ $\forall i, j\ için\ 1 \leq i \leq j \leq r\ olmak$ üzere $(m_i, m_j) | (a_i, a_j)\ dir.$ Eğer bu lineer kongrüans sisteminin $M = m_1, m_2, \ldots, m_r\ moduna\ göre$ bir çözümü mevcut ise bu çözüm tektir. Bu teoreme Genelleştirilmiş Çin Kalan Teoremi adı verilir.

Teorem 1.7.7: $a \neq b$ olsun. Bu iki tamsayı aralarında asaldır ↔ $ax + by = 1$ eşitliğini sağlayan $a, b \in Z$ vardır.

1.8. Kriptolojinin Tarihçesi

Kriptolojinin en eski örneğine M.Ö. 1900 de Mısırlılar'ın yazdığı kitabelerde rastlanmaktadır.



Şekil 1. 8. Mısır'ın Reşid kasabası yakınında yapılan kazıda bulunan Rosetta taşı [29]

Daha sonra İbranilerin kutsal kitaplarında ki belirli kelimelerde şifreleme görülmüştür. M.Ö. 300 de Kautilya tarafından Hindistan'da yazılmış bir kitap olan Artha-Sastra çeşitli kriptanaliz yöntemlerini önerir.

M.Ö. 60–50 yıllarında Julius Caesar tarafından devlet iletişiminde tercih edilen ve alfabedeki harflerin belirli bir sistematik yapıyla yerlerinin değiştirildiği bir şifreleme metodu geliştirmiştir. Bu şifreleme yöntemi, iletilecek olan verideki her bir harfin alfabede kendisinden üç harf sonraya kaydırılmasıyla oluşturulan ve "Sezar Şifrelemesi" olarak bilinen şifreleme yöntemidir.

725–790 yıllarında İlk Arap sözlüğünün de yaratıcısı da olan Abu Abd al-Rahman, Bizans imparatoru için Yunanca yazılmış bir şifreli metni çözmeyi ilham alarak oluşturduğu ve kitap kriptografi üzerine kurulmuş olan kitaba günümüzde ulaşılamamaktadır.

1000–1200 yılları arasında Gazneliler' in yazdığı bazı şifreli dokümanlar, günümüze kadar gelmiştir.

1586'da Blaise de Vigenère, ilk kez açık metin ve şifreli metin için otomatik anahtarlama sisteminin anlatıldığı bir kitap yazdı. Günümüzde bu yöntem hala DES, CBC ve CFB tiplerinde uygulanmaktadır.

1623'de Sir Francis Bacon, stenografı bulmuştur. Meclis oturumlarında, mahkeme duruşmalarında, iş görüşmelerinde oldukça yaygın bir şekilde kullanılan Stenografi, alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan çabuk yazma sistemidir. Yazılar yakın, küçük ve dar yazıldığı için bu adı almıştır.

1790'de Pensilvanya Üniversitesi'nde matematikçi olan Thomas Jefferson Wheel, (tekerlek) şifresini icat etti. Bu durum M-138-A Strip Cipher makinesinin gelişmesine yol açtı.

1854'de Charles Wheatstone, playfair şifresini bulmuştur.

1861'de Friedrich W. Kasiski, tekrar eden harf gruplarını kullanarak çok alfabeli şifrenin ilk genel çözümünü veren ve yıllarca güçlü kabul edilen çok alfabeli şifrenin artık zayıf olarak kabul edilmesine sebep olan bir kitap yayınladı.

1914 de 1. Dünya Savaş'ı başlamasıyla birlikte güçlü bir askeri kriptografisi kullanılmıştır. Sürekli gelişim göstererek de her iki dünya savaşının sonucunda da önemli bir rol oynamıştır.

1919'da Joseph Mauborgne ve Gilbert Vernam, mükemmel şifreleme sistemi olarak bilinen "one-time pad" şifreleme sistemini oluşturmuşlardır.

1920 ve 1930'larda FBI, bir araştırma ofisi kurdu. Bu ofisin amacı, içki kaçakçılarının aralarında ki iletişimi deşifre edebilmekti. William Frederick Friedman tarafından kurulan Riverbank Laboratuarları, Amerika Birleşik Devleti için kriptotolojik sistemlerin analizini yapmış ve 2. Dünya Savası'nda Japonlar'ın kullandığı Purple Machine, kriptolojik sistemi deşifre etmiştir.

1952'de Amerikan Hükümeti kriptoloji biliminin ne kadar önemli olduğunun farkında olduğundan dolayı NSA'yı oluşturmuşlardır. NSA, ABD'de de resmi olarak ulusal güvenlik teşkilatı olarak kabul edilen yapıdır.

1970'de Horst Feistel (IBM), DES' in ana unsuru olan Lucifer algoritmasını geliştirmiştir. ABD ileri teknoloji enstitüsü NIST tarafından geliştirilen DES, tarihte en iyi bilinen sistemdir.

1976'da DES, ABD tarafından FIPS 46 standardı olarak açıklanmıştır.

1976'da Whitfield Diffie ve Martin Hellman, açık anahtar sistemini anlattıkları "New Directions In Cryptology" adlı makaleyi yayınlamışlardır. Böylelikle Açık Anahtarlı Kriptografi doğmuştur. Bu makale, kriptolojide bir dönüm noktası olmuştur. Yayınladıkları makale ile anahtar değişimi problemine çözüm getirmişlerdir. Geliştirdikleri yöntemle istenilen güvenilirliği sağlayamayan anahtar dağıtım merkezlerine olan gereksinimi ortadan kaldırmıştır. Bu şekilde anahtarın dağıtım merkezindeki üçüncü şahısların eline geçme riskini ortadan kaldırmışlardır.

1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman, RSA (Rivest-Shamir-Adleman) algoritmasını bulmuşlardır. Başka bir deyişle ilk pratik açık anahtar şifreleme ve imza tasarısını keşfetmişlerdir.

1985 yılında da El Gamal tarafından diğer bir güçlü ve pratik açık anahtar tasarısı bulunmuştur.

1985'de Neal Koblitz ve Victor S.Miller, ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif etmişlerdir.

1990'da Xuejia Lai ve James Massey, uluslararası veri şifreleme algoritması olan IDEA algoritmasını bulmuşlardır.

1991'de Phil Zimmerman isimli kişi, şifreleme sistemi olarak, PGP' yi geliştirmiş ve yayınlamıştır.

1995'de 'Güvenli Özetleme Algoritması' olarak bilinen SHA–1, NIST tarafından standart olarak yayınlanmıştır.

1997'de ABD'de NIST, DES'in yerini alacak bir simetrik algoritma için yarışma açmıştır.

1998'de Lee ve Chang, şifreleme işlemlerinde hızı artırabilmek için küçük ortak anahtarı daha büyük seçebilecek bir yöntem önermişlerdir.

2001'de NIST' in düzenlediği yarışmayı kazanan Belçikalı Joan Daemen ve Vincent Rijmen oldu. Bu kişilerin oluşturduğu ve yarışmayı kazanmalarını sağlayan Rijndael algoritması, yeni ismi AES ile standart haline getirildi.

2005'de SHA–1 algoritmasının Çin'li bir ekip tarafından deşifre m edildiği ve gücünün 2^{80} den 2^{63} e kadar düştüğünü duyurmuşlardır. Bunun üzerine bu algoritmayı kullanan Microsoft, Sun gibi birçok büyük firma artık bu algoritmayı bundan sonraki süreçte tercih etmeyeceklerini açıklamışlardır.

2009'da kriptografi konusunda dünyanın ilk olimpiyatları için Belçika'nın Katholieke Üniversitesinde bir ön eleme düzenlendi. 25–28 Şubat tarihleri arasında yapılacak olan

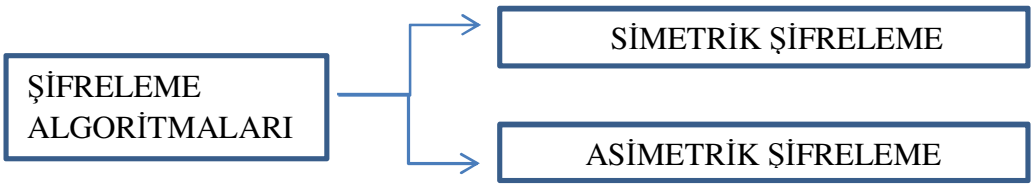
bu ön eleme ile başlama sürecine giren bu olimpiyatların amacı, SH1'lerin Çin'li ekip tarafından çözülmesinden sonra yeni ve eskisine göre daha güvenli bir algoritmanın oluşturulmasıydı.

Şifrelemenin tarihçesi genel hatlarıyla bundan ibarettir [2, 6, 11, 12, 15, 25, 29]. Şimdi gelelim şifreleme algoritmalarına:

2. BÖLÜM

GENEL ŞİFRELEME ALGORİTMALARI

Şifreleme ve deşifreleme işlemleri için birtakım yöntemler kullanılmaktadır. Bu kullanılan yöntemlere kriptografik algoritmalar adı verilir. Günümüzde kullanılan kriptografik algoritmalar anahtarlı ve anahtarsız olmak üzere iki farklı metot üzerine inşa edilmiştir. Sıkıştırma fonksiyonları, hash fonksiyonları anahtarsız metoda örnek iken anahtarlı metotlarda ise kullanılan anahtarın özellikleri ve çeşidine göre simetrik veya asimetrik algoritmalar olarak adlandırılırlar [7, 27].



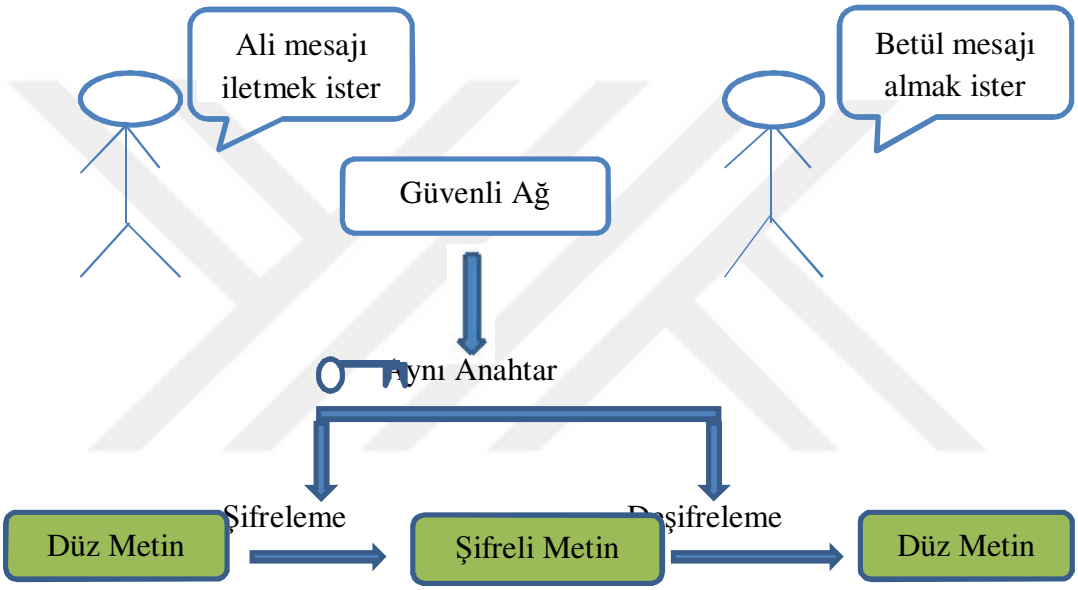
Şekil 2. 1. Genel şifreleme algoritmaları

2.1. Simetrik Şifreleme Algoritması

Diğer bir adıyla gizli anahtarlı şifreleme olarak bilinen simetrik şifreleme algoritması, bilginin başkası tarafından okunamayacak bir forma dönüştürülmesi ve şifreli hale getirilen bilginin sadece alıcısı tarafından çözülmesi işlemi için aynı anahtarın tercih edildiği algoritma türüdür [20]. Bu anahtar, sadece iletilecek olan metni şifreleyecek ve şifrelenmiş olan metinde deşifreleme işlemini gerçekleştirecek olan şahıslarda bulunmaktadır ve bu anahtar başkalarından gizlidir. Yani düz metne erişmek için gizli

anahtarın bilmek gereklidir. Karşı tarafa ulaşması istenen gizli metin, taraflar arasında anlaşılmış olan gizli anahtar ile birlikte alıcıya gönderilir ve deşifreleme işlemi gerçekleştirilir [23].

Bu noktada, güvenli anahtar dağıtım kısmında problemler yaşanmaktadır. Bu sistemin güvenliği ile şifreleme yapmak için oluşturulan anahtarın kaba kuvvet yöntemi uygulanarak şifreli metni kırma işlemi ile ilişkilidir. Genel şeması:



Şekil 2. 2. Simetrik şifreleme algoritmasının ana yapısı

İkiye ayrılır. Bunlar:

1. Blok şifreleme algoritmaları

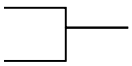
2. Akan Şifreleme algoritmaları [4, 9, 23]

Örnek olarak:

1. AES
2. DES
3. IDEA
4. 3DES
5. Skipjack
6. RC5
7. Camellia
8. Blowfish

(Blok Şifrelemeye örnek)

9. RC4
10. RC2



(Akan Şifrelemeye örnek)

Tablo 2. 1. Simetrik şifreleme yöntemleri, çıkış tarihi ve geliştiren kişiler [22]

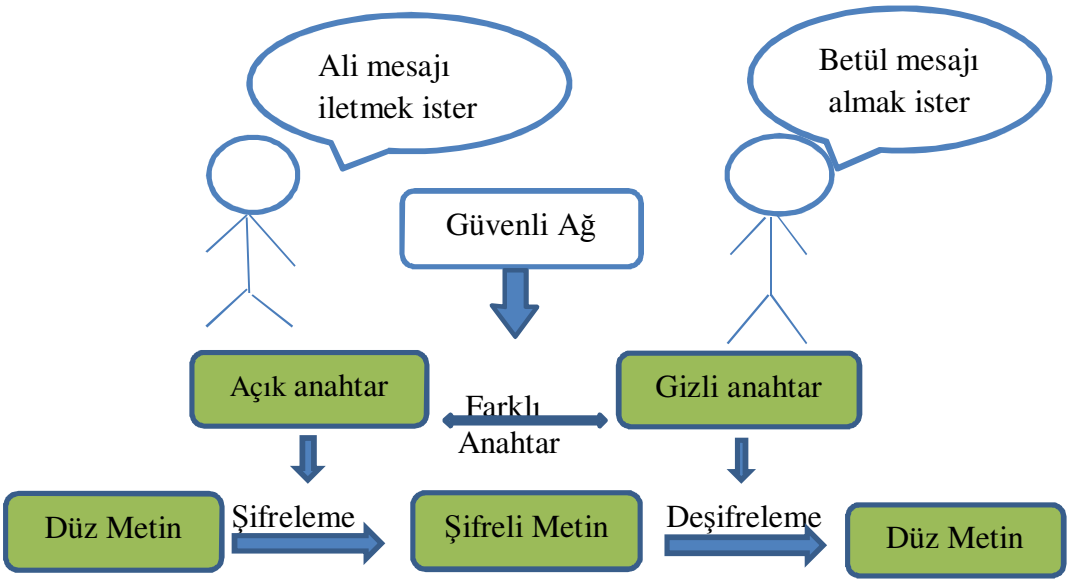
Şifreleme Yöntemi	Ortaya Çıktığı Yıl	Geliştiren Kişi
DES	197	IBM
3DES	1978	IBM
RC2	1992	Ron Rivest
IDEA	1992	Xuejıa Lai ve James Massey
SKİPJACK	1993	NSA
BLOWFİH	1993	Bruce Schneier
RC5	1995	Ron Rivest
AES	1997	Joan Daemen ve Vincent Rijmen
CAMELLİA	2000	NTT ve Mitsubishi Electric Corporation

1970 lere kadar kullanılan şifreleme metodu AES ve DES olmasından yapacağımız çıkarım bu yıla kadar bütün kriptolojik yapının simetrik olmasıdır.

2.2. Asimetrik Şifreleme Algoritması

İlk olarak Whitfield Kiffie ve Matin Hellman' ın ortaya attığı Asimetrik algoritma ise simetrik algoritmalardan farklı olarak şifreleme ve deşifreleme işlemlerinde ayrı ayrı anahtarın kullanıldığı algoritmalardır. Şifrelemede kullanılacak olan anahtarın halka açık olmasından dolayı bu şifreleme algoritmasına açık anahtarlı algoritma da denir [20]. Asitmerik şifrelemede her iki tarafın sahip olduğu açık anahtar ve gizli anahtar olmak üzere bir anahtar çifti kullanılır [23]. Fakat bu anahtar çifti birbiriyle matematiksel olarak ilişkilidir. Başka bir deyişle gizli anahtar, matematiksel bir algoritma ile açık anahtardan bulunur [2, 13]. Mesela telefon ortamındaki haberleşme programlarını ele alalım. Deşifreleme işlemi için ihtiyaç duyulan gizli anahtar alıcısına asimetrik şifreleme yoluyla iletilir. Bu aşamadan sonra ise iletilen bu anahtarla simetrik şifreleme yöntemine başvurularak aradaki iletişim yani mesajlaşma sağlanır. Burada ki

ana mantık birbirini daha önceden hiç tanımayan kişilerin bile bu metotla gizlice haberleşmesidir. Şifreleme anahtarı olarak kullanılan anahtarın gizli olması gerekmez [23]. Halka açıktır. Bu açık anahtarla şifrelenen mesaj sadece alıcıdaki gizli anahtarla çözülebilir ya da işlemi tersine düşünecek olursak alıcının özel anahtarıyla attığı sayısal imzanın doğrulanması göndericideki açık anahtarla mümkündür. Örneğin Ahmet sertifika yöntemiyle güvenilirliği ve gerçekliği ispatlanmış bir internet sitesi üzerinden online alışveriş yapacak olsun. Girdiği siteden temin ettiği halka açık anahtarla kimlik bilgisi, kullanacağı kart bilgilerini şifreleyerek satıcıya ulaştırır. Bu sayede üçüncü bir kişi tarafından, siteye verdiği kişisel bilgilere ulaşılmasına engel olmuş olur. Şifreyi de sadece alışveriş yaptığı sitenin sahibi olan satıcı çözebilir. Sonuç olarak ta güvenli bir şekilde alışveriş tamamlanmış olur [27]. Bu şifreleme metodunun altında yatan temel düşünce, açık anahtar verildiği halde deşifreleme anahtarı olarak kullanılan anahtarın bulunmasının zor olmasıdır. Bu şifreleme metodunda fonksiyonun birebir olduğu bir aralık tercih edelim. Seçilen bu aralıkta fonksiyonu hesaplamak kolayken tersinin hesaplanması mümkün değildir. Örneğin RSA Şifreleme Metodu'nda çok büyük iki asal sayı seçilerek yapılan bir takım matematiksel işlemler sonucu anahtar oluşturma, oluşturulan anahtarı kullanarak şifreleme yapma işlemi kolaydır. Ama deşifreleme yapılırken matematiksel işlemlerden biri olan iki büyük asal sayının çarpımı işleminin tersini bulmak oldukça zordur.



Şekil 2. 3. Asimetrik şifreleme yönteminin ana yapısı

Açık anahtarlı algoritmalar bazı işlemlerin hesapsal olarak kolay olmasını gerektirdiğinden dolayı geçmişten günümüze sunulan bu algoritma türlerinden sadece bir kaçı geniş kitlesel olarak kabul görmüştür. Asimetrik şifreleme algoritması olarak önerilen bu algoritmaları şunlardır:

1. RSA
2. El Gamal
3. Eliptik Eğri Sistemleri
4. Diffie-Hellman anahtar belirlemesi
5. Kod-Tabanlı Kriptosistemler [4, 23].

Tablo 2. 2. Asimetrik şifreleme Yöntemleri, Çıkış Tarihi Ve Geliştiren Kişiler [22]

Şifreleme Yöntemi	Ortaya Çıktığı Tarih	Geliştiren kişi
DİFFİE-HELLMAN	1976	Diffie ve Hellman
RSA	1978	Ron Rivest, Adi Shamir ve Leonard Adleman
EL-GAMAL	1985	El Gamal
ELİPTİK EĞRİ SİSTEMLERİ	1987	Koblitz

Bu algoritmalar içerisinden kullanım olarak en çok tercih edilen algoritma RSA'dır. RSA kriptolojik sisteminin analizi, asal sayılara ve deşifrelemenin çarpanlara ayırmaya bağlı olması bu algoritmanın üçüncü şahıslar tarafından kırılma ihtimalini zora sokacağından dolayı günümüzde hala kullanımı yaygın olan bir algoritmadır [25].

2.3. Sayısal İmza

Kriptolojide veriyi güvenli bir şekilde saklamak ya da alıcısına iletmek esas amaçtır. Buna göre bilgi alınır ve gerekli anahtarlar yöntemiyle şifrelenerek karşı tarafa ulaştırılır. İşte tam da bu noktada sayısal imzalar devreye girer. Bilgisayar ortamında kimlik belirticisi olan sayısal imza, sanal olmayan ortamdaki mevcut evraklardaki atılan

imzalar kadar bağlayıcı olan bir teknolojidir. Elektronik imzada denilen sayısal imzaların İngilizce karşılığı 'Digital Signature' dir. Teknolojide artar hızın yüksek güvenlik gereksinimini beraberinde getirmesiyle birlikte, saldırı yapmak için bekleyen tehdit unsuru olan kötü niyetli kullanıcılar yaptığı saldırılarla asıl mesajı alacak olan kişilerin mutlaka tanıtılmasını gerekli kılmıştır. Buradan da anlıyoruz ki sayısal imzalar mesajı alacak olan kişilerin bilgilerini doğrulamak amacıyla tercih edilir. Sayısal imzalardan yararlanılarak veriyi şifreli olarak alacak olan kişi, şifreyi gönderecek olan kişinin kimliğinin doğrulamasını yapar. Bu sayede şifreli metni gönderen asıl kişinin kim olduğundan emin olur. İkinci bir aşama ise sayısal imzadaki amaç gönderici hangi veriyi şifreleyip gönderdi ise o verinin bütünlüğünün alıcı tarafından kontrolüdür. Gönderici, şifreli metni göndermediği halde yolladığını söyleyemez. Buradan şunu söyleyebiliriz ki bu teknoloji veriyi gönderen kişinin kimlik tespitinde ve gönderilen verinin bütünlüğünün sınanmasında kullanılır [7].

Gerçek el imzasının amacı ne ise sanal ortamda gerçekleştirilen sayısal imzada aynı amacı taşımaktadır. İkisinin arasındaki fark ise el imzasını taklit edip kullanmak kolaydır ancak sanal imzanın taklidi zordur. Hatta neredeyse taklit edilmesi mümkün değildir.

Hızla gelişen teknolojiyle birlikte kriptolojide güvenlikte önem kazanmıştır. Gerekli güvenliğin sağlanması için yapılan gelişmeler, sayısal imzalarında yasallaşmasına yönelik yapılan çalışmalara öncü olmuştur.

Bahsi geçen bu sayısal imzalama asimetrik şifreleme sistemi yardımı ile yapılır ve PKI adı verilen açık anahtar altyapısının en önemli noktasını oluşturur.

Islak imzanın bilgisayar ortamındaki bir başka deyişle bilişim dünyasındaki karşılığı olan sayısal imzalar aşağıdaki bazı önemli unsurları sağlar. Tanım 2.3.1. , 2.3.2. ve 2.3.3. kısımları kaynak [7] den alınmıştır.

2.3.1. Tanıma

Bir nevi kimlik doğrulama işlemidir. İşlemi bir kişi, firma, sunucu her kim gerçekleştirdi ise onun kimliği onaylanır. İşlemi kimin yaptığı, işlem boyunca mevcut katılımcıları, iletilmek istenen bilgiye başkasının müdahalesi olup olmadığını tespit eder. Mesajı gönderen kişinin doğru kişi olup olmadığının anlaşıldığı aşamadır.

Bununla alıcı mesajın aslında kim tarafından gönderildiğini herhangi bir saldırıya uğrayıp uğramadığının tespitini yapmış olur.

2.3.2. Gizlilik ve veri doğruluğu

Sayısal imzada amaç bilginin alıcısına hiçbir şekilde değiştirilmeden, her hangi bir saldırıya maruz kalıp bozulmadan ulaştığını ispatlamaktır. Kriptolojide veri bütünlüğü, verinin gizliliği ve verinin olduğu gibi karşı tarafa ulaşması esastır. Veri gizliliği ve bütünlüğü sağlanarak iletilmek istenen metnin sadece alıcısı tarafından çözülüp okunması, işte bu sayısal imza ile mümkündür.

2.3.3. İnkâr edememe

Sayısal imzada tanıma faktörü sayesinde kimlik tespitine olanak sağlar. Bu sayede şifreleme işlemi sırasınca işleme kimler katılmış kanıtlanabilir. Bunu kanıtlanmasıyla da gönderici ve alıcı arasında inkâr edememe durumu söz konusu olur. Yani ne gönderici veriyi göndermediği halde gönderdim diyebilir, ne de alıcı veriyi aldığı halde almadığını iddia edebilir.

Sayısal imzalar da güvenlik açısından üç ayrı hizmet söz konusudur.

1. İmzalanacak olan verinin güvenilir olması.
2. İmzalanacak olan verinin alıcısına ulaşacağı zamana kadar bütünlüğünün korunması.
3. İmzalanacak olan verinin alıcısına ulaşacağı ana kadar üçüncü kişiler tarafından kopyalanmasını engellemek. Sayısal imzaların bazı uygulamalarına

- Diffie-Hellman
- Merkle-Hellman
- RSA
- El Gamal

örnek verilebilir.

Sayısal imzalar sayısal sertifikalardan yararlanılarak oluşturulur ve yine sayısal sertifikalardan yararlanılarak onaylanır. O halde sayısal sertifika nedir bir göz atalım.

2.4. Sayısal Sertifikalar

Gelişen teknolojiyle birlikte internet ortamında alış veriş artmış, böylelikle de ticari faaliyetler artış göstermiştir. Bu da internet ortamında da bir takım güvenlik

unsurlarının sağlanmasını gerekli kılmıştır. Sayısal imzalar ve sertifikalar bu unsurlardan bir kaçıdır. Sanal ortamlarda yapılan ticari faaliyetlerde internet sistemini kullanmaya yetkili olduğuna dair verilen belgeye verilen ad sayısal sertifikadır. Kriptolojide ise sayısal sertifika, mevcut onay kurumu tarafından elektronik ortamda hazırlanıp imzalandığı belgelerdir. Dijital sertifikalar ya da açık anahtar sertifikası da denir. Bu belgede şifreleme yapmak için kullanılacak olan açık anahtarların kimlere ait olduğu gösterilir. Alıcısına ulaşan metin, gerçekten istenilen kişi tarafından mı gönderildi ya da ulaşan metin orijinal metin mi herhangi bir saldırıya, bu saldırı sonucunda da herhangi bir değişikliğe uğramış mı sorularının cevabı sayısal imzalarla karşılanır. İşin bir de şifrelenerek oluşturulmuş mesajın asıl alıcısına ulaşıp ulaşmadığı boyutu vardır. Bu da sayısal sertifikalar sayesinde netlik kazanır. Certificate Authority tarafından hazırlanan sayısal sertifikaların güvenilirliği, sertifikaları numaralandırmak için kullanılan rakamların artışıyla doğru orantılıdır. Sayısal sertifikalar

1. Class 0
2. Class 1
3. Class 2
4. Class 3
5. Class 4

olmak üzere beş kısımda sınıflandırılır [14].

2.5 Simetrik Şifreleme Algoritması ve Asimetrik Şifreleme Algoritmasının Karşılaştırılması

Simetrik algoritma ve asimetrik algoritmaların kendi içlerimde avantajları ve dezavantajları vardır. Bu iki algoritmayı karşılaştıracak olursak:

Simetrik şifreleme sisteminin diğer algoritmalara göre en önemli avantajlarından birisi diğerlerine kıyasla oldukça hızlı olmasıdır. Özellikle asimetrik şifreleme metoduyla hız açısından karşılaştırıldığında, simetrik algoritmalar daha ön plandadır. Çünkü asimetrik algoritmalarda güvenliği yüksek tutabilmek için seçilen asal sayıların çok büyük olması, zaman açısından değerlendirildiğinde asimetrik algoritmayı dezavantajlı duruma getirmektedir. Bazı donanımsal uygulamalar saniyede yüzlerce megabyte veri şifreleme görevini başarabilirken, bu yazılımsal uygulamalarda saniyede megabyte'lar düzeyinde gerçekleşir. Ayrıca simetrik algoritmaları basit işlemler içerdiği için elektronik

cihazlarda uygulamak daha kolaydır ya da bir başka deyişle asimetrik şifreleme yönteminde çok büyük asal sayıların tercih edilmesinden dolayı donanımsal yapılara uyum sağlaması oldukça zor olmaktadır. Özellikle kablosuz ağ sistemlerinde bu algoritmanın kullanılması, bazı sorunlara yol açabilir. Çünkü bant genişliğini fazlaca tüketir ve sistemi yavaşlatarak performans düşüşüne neden olur.

Simetrik şifreleme algoritmalarında bulunan en büyük problem ise simetrik algoritma kullanan çok kullanıcılı bir sistemde, bütün kullanıcılara aynı anahtarın dağıtılması güvenlik açısından problemli olabilir. Her kullanıcıya farklı bir anahtar vermek ise sistemde birçok farklı anahtar gerektireceği için problemli olabilir. Bu sorunları çözüm getirmek için asimetrik şifreleme algoritmaları geliştirilmiştir. Asimetrik (açık anahtarlı) şifreleme ile ilgili ilk düşünceler ortaya atılana kadar kullanılan simetrik şifreleme yöntemi göz önünde bulundurulduğunda, açık anahtarlı şifreleme metodunun gelişmesi, bütün kriptografi tarihindeki en büyük devrimdir. İkinci dünya savaşında şifreleme ve deşifreleme yapan rotor makinelerinin var olmasıyla, geleneksel kriptografide büyük bir adım atılmış ve elde edilen bu gelişme temelleri 1970'li yıllara dayanan asimetrik şifrelemenin önünü açmıştır. Simetrik şifrelemedeki anahtar paylaşım sorununu çözmek için 1976'da Whitfield Diffie ve Martin Hellman tarafından asimetrik şifreleme tekniği geliştirilmiştir. Geliştirilen bu yeni şifreleme tekniği sayesinde dijital verilerin gizliliği önem kazanmış, özellikle internetin iş ve özel hayatta vazgeçilmez bir hâle gelmesiyle de bu önem daha da artmıştır. Bu yöntemde iki ayrı anahtar kullanılması ve herhangi bir anahtar transferinin gerekmemesi güvenliği artırmaktadır. Asimetrik şifreleme algoritmalarında şifreleme anahtarı ile şifrelenmiş veriyi çözmek için kullanılan anahtar birbirinden farklı olduğu için güvenilirlik açısından simetrik algoritmalardan daha başarılıdır. Ayrıca asimetrik şifreleme algoritması az sayıda anahtar kullanarak simetrik şifrelemede büyük sıkıntı teşkil eden anahtar fazlalığı durumunu engeller. Ayrıca simetrik şifreleme anahtarın güvenlik açısından sık sık değiştirilmesi gerekirken, açık anahtar kriptolamada anahtar çiftinin uzun süre değiştirilmesine ihtiyaç yoktur. Ancak anahtar uzunluğu bakımından karşılaştıracak olursak simetrik anahtar şifrelemede açık anahtar şifrelemeye göre nispeten daha kısa şifreleme anahtarları tercih edilir. Aşağıdaki tabloda Asimetrik ve simetrik kriptografi sistemlerinin özellikleri karşılaştırılmıştır.

Tablo 2. 3. Simetrik kriptografi ve asimetrik kriptografinin özellik sağlaması açısından karşılaştırılması [1, 20]

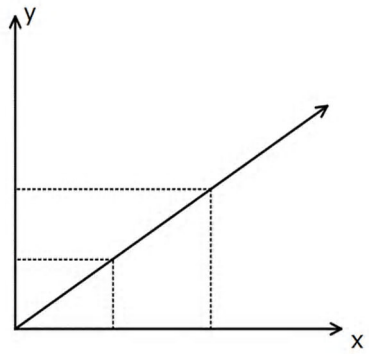
KONU	SİMETRİK ŞİFRELEME SİSTEMİ	ASİMETRİK ŞİFRELEME SİSTEMİ
Gizlilik	Özelliğe sahip	Özelliğe sahip
Bütünlük	Özelliğe sahip değil	Özelliğe sahip
Kimlik Doğrulama	Özelliğe sahip değil	Özelliğe sahip
İnkâr Edememezlik	Özelliğe sahip değil	Özelliğe sahip
Performans Hızı	Yüksek	Düşük
Güvenlik	Anahtar Uzunluğuna Bağlı	Anahtar Uzunluğuna Bağlı
Anahtar Sayısı	Tek Anahtar	Çift Anahtar
Anahtar Boyutu	Düşük	Yüksek

2.6. Hybrid şifreleme

Günümüzde bu iki şifreleme algoritmalarını bir arada kullanarak hem son derecede güvenliğe sahip hem de hızı yüksek sistemlere şifreleme işlemi uygulanabilmektedir. Bu gibi sistemler hybrid şifreleme yöntemi adını alır. Burada ki amaç, her iki algoritmanın da zayıf yönlerini arkada bırakarak bu şifreleme yöntemlerinin güçlü yönlerini kullanarak, şifrelenip iletilecek ya da saklanacak olan bilginin güvenliğini ve şifreleme hızını artırmaktır. Anahtarla şifreleme, anahtar ile anlaşma ve elektronik imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemi ve imza gerektirmeyen verilerin bütünlüğünü koruma işlemi ise simetrik şifreleme ile gerçekleştirilir. Bunun en güzel örneği PGP' dir. Burada amaç, birbirlerinin yerine geçmek değil aksine birbirlerini tamamlayarak yapıyı daha güvenli bir hale getirmektir [26].

3. BÖLÜM
RSA ŞİFRELEME ALGORİTMASI

Diffie ve Hellman, şifreleme yönünde hesaplanması kolay iken deşifreleme yönünde elde gerekli bilgiler var olmadan hesaplanmasının oldukça güç olduğu, tek yönlü ve arka kapılı fonksiyonlar ile asimetrik kriptoloji sistemleri önermesinde bulunmuştur [10]. Bu fonksiyonları kullanarak asimetrik şifreleme sisteminin ilk örneği olan RSA'nın geçmişine göz atacak olursak; 1978 yılında R. Rivest, A. Shamir ve L. Adleman tarafından geliştirilmiş, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" isimli makalede yayınlan, geliştiricilerinin soyadlarının baş harfleri olan RSA olarak ifade edilen sistem, 4405829 nolu 1983 de Amerika'da mitten alınan ve 21 Eylül 2000 de son bulan Patent ile korunan ve en çok kullanılan açık anahtarlı şifreleme sistemidir [18]. Bu yöntemin temel mantığı ise 1973 yılında C. Cocks aracılığı ile öne sürülmüştür. Birleşik Krallık haber alma teşkilatında çalışan ve bir İngiliz matematikçisi olan Clifford Cocks, 1973'te bir sistem açıkladı. Bu sistem, ileri yönlü çok hızlı çalışan ama sistemi geri çevirirken çok çok yavaş çalışan bir sistemdi ve bu sistemi çalıştırabilmek için çok donanımlı ve pahalı bilgisayarlara ihtiyaç duyuldu ve bu ihtiyaçlar temin edilemediğinden dolayı bu sistem hiç uygulanamadı. Bu buluş çok gizli olduğu içinde 1998 yılına kadar açığa çıkarılmadı. İşte tam bu noktada **R**ivest, **S**hamir ve **A**dleman, Cocks'un buluşundan bağımsız olarak RSA şifreleme yöntemini tasarladılar. RSA hem şifreleme hem de sayısal imza atma olanağı tanıyan bir kriptografik yapıdır. Aynı zamanda public-key şifreleme metodunun temel bir uygulaması olan RSA şifreleme yönteminin güvenliği, çarpanlara ayırma probleminin zorluğuna dayanmaktadır [27]. Yani temel mantığı seçilen çok büyük ve asal olan iki sayının çarpılmasıyla yeni bir tamsayı oluşturma yöntemine dayanan RSA Şifreleme Sistemi'nin güvenli olması, ilk başta seçilen asal sayıların büyüklüğü ile doğru orantılıdır. Bu durum RSA için bir avantaj iken şifreleme ve deşifreleme de yavaş kalması en büyük dezavantajlarındandır [7, 20].



Şekil 3. 1. RSA güvenilirliği ile seçilen asal sayıların büyüklüğü arasındaki ilişki
x: RSA şifreleme yönteminin güvenilirliği
y: Seçilen asal sayıların büyüklüğü

Modern kriptolojinin 1970□lerden sonra ilerleme göstermesiyle birlikte tamsayıları çarpanlarına ayırma sorunu, deşifreleme işlemi için çok önemli bir konu haline gelmiştir. Bu problemi ortadan kaldırabilme adına geçmişte ismi sıkça duyulmuş olan Fermat, Euler, Legendre, Gauss gibi ünlü matematikçiler, tamsayıların çarpanlarına ayrılması ile ilgili çeşitli çalışmalar yapmıştır [6].

Şimdi RSA nın yapısını inceleyecek olursak: RSA ile yapılacak olan metin şifreleme işleminde ilk olarak şifrelemede kullanılacak olan anahtar oluşturulur. Seçilen anahtarlar yeteri kadar uzun olduğunda güvenli olduğu düşünülür. Örneğin Romalılar, 2009 yılında yapılan bir çalışmada 232 basamaklı bir sayıyı (RSA-768), yüzlerce makinayı iki yıl boyunca çalıştırarak çarpanlarına ayırmışlardır. Haberleşmede yer alacak kişiler, bir RSA açık anahtarı ve buna karşılık gelen özel anahtarı oluşturur. Önceden aralarında hiçbir iletişim olmayan alıcı ve vericinin, kendi aralarındaki iletişimin güvenli bir ortamda yapılması, bu algoritmanın başka bir avantajıdır. Açık anahtar herkesle paylaşılabilir. Şifreleme işlemini gerçekleştirmek isteyen kişi, seçilen bu açık anahtarı kullanarak karşı tarafa ulaştırmak istediği metni şifreler ve iletişim kurmak istediği kişiye bu şifreli metni gönderir. Ancak gizli anahtarı kim biliyor ise deşifreleme işlemini de ancak o gerçekleştirebilir.

3.1. RSA Algoritmasının Özellikleri

1978 yılında karşımıza çıkan RSA şifreleme yönteminde ön koşul, seçilen çok büyük asal sayılarla birlikte şifrelemede yararlanacağımız bir anahtar oluşturmaktır. Halka açık olan anahtar ve sadece alıcısında olan gizli anahtarlarda gerekli güvenliği sağlayabilmek adına seçilen boyut, 1024 bitten büyük olmalıdır. Boyutun bu kadar büyük seçilmesi, güvenlik açısından avantaj iken şifreleme, bu anahtar üzerinden bazı matematiksel algoritmalar gerektireceğinden zaman alıcı olacaktır. Tersine şifreli metni çözme işleminde de bu sefer karşımıza çarpanlara ayırma zorluğu geleceğinden deşifreleme de zaman alacaktır. Halka açık olan ve herkesten gizli tutulan anahtar olmak üzere iki anahtar çifti barındıran bu algoritmanın başlama hızı ise hızlı olacaktır [22].

Tablo 3. 1. RSA' nın genel özellikleri [22]

Özellikler	RSA
Tarihi	1978
Anahtar Uzunluğu	> 1024 bit
Blok Uzunluğu	≥ 512 bit
Şifreleme ve Şifre Çözme İşlemi için Kullanılan Anahtar	Birbirinin aynısı değil
Algoritma Türü	Asimetrik Şifreleme sistemi
Şifreleme işleminin Hızı	Düşük hız
Şifre Çözme işleminin Hızı	Düşük hız
Güç Tüketimi	Yüksek
Güvenilirliği	Oldukça güvenilir
Kullanılan Anahtar	İki farklı anahtar kullanılır.
Devir Sayısı	1
Başlama Hızı	Hızlı

3.2. RSA nın Tarihi

RSA' nın yakın tarihine de söyle bir göz atacak olursak;

RSA, dünyada meydana gelen birçok problemlerde ve mühendisliğin çeşitli alanlarında kullanılmaktadır. Özellikle son yıllarda bu algoritmayı göz önünde tutan çok sayıda çalışma bulunmaktadır.

2010 yılında Somani vd. , RSA algoritmasını Bulut bilişimde verilerin güvenliğini geliştirmek için tavsiye etmişlerdir.

2012 yılında Dubey vd. MD5 ve RSA algoritmasını kullanarak Bulut kullanıcısı ile bulut sağlayıcısı için verilerin toplanması ve toplanan bilgilerin paylaşılmasına yönelik güvenilirliği yüksek bir sistem oluşturduklarını ve oluşturdukları bu sistemle de daha güvenilir hesaplama işlemlerinin gerçekleştirilebileceğini söylemişlerdir.

2013 yılında Patidar ve Bhartiya tarafından önerilen RSA Şifreleme Sistemi'ni hızlandırmaya yönelik tasarlanan modifiye edilmiş RSA algoritmasında normal RSA da ki gibi anahtar oluşturmak için kullanılan iki asal sayı yerine üç asal sayı kullanmayı tercih etmişlerdir. Bununla şifreleme algoritmasının hızını ve güvenliğini artırmaya yönelik çalıştıklarını söylemişler ve orijinal RSA ile önerdikleri bu sistemi kıyaslamışlardır. Yapılan karşılaştırma sonuçlarına göre ise önerilen algoritmanın orijinal RSA'dan daha güvenilir olduğunu beyan etmişlerdir.

Yine 2013 yılında Ayele ve Sreenivasarao'nın RSA şifreleme sistemi için önerilen iki ortak anahtarlı bir yöntemde, bahsi geçen bu iki ortak anahtarın ayrı ayrı karşı tarafa iletilmesi, bu sisteme karşı yapılabilecek olan saldırıları düzenleyenin oluşturulan anahtar ile igili çok fazla bilgi sahibi olmamasına ve şifreli metinde şifrenin deşifre edilememesine neden olduğunu ileri sürmüşlerdir. Ayrıca öne sürülen bu RSA'nın daha düşük bir hız ile güvenilirliği yüksek bir sisteme olanak sağladığını söylemişlerdir.

2014 yılında Jaiswal vd. , belirli bir sistem ağı üzerinden gerçekleştirilen verinin alışverişi sırasında geçen sürenin kısalması ve yüksek güvenlikli olması için modifiye edilmiş olan RSA Şifreleme Sistemi'ni önermişlerdir. Orijinal RSA ile önerilen RSA'nın kıyasının yapılması sonucunda tavsiye edilmiş olan RSA'nın, orijinaline göre daha yüksek güvenlik sağladığı ve şifreleme sırasında geçen zamanın kısaltıldığı neticesine ulaşılmıştır.

2015 yılında Thangavel vd. , RSA Şifreleme Algoritması üzerinde bir takım değişiklik yapmış ve daha gelişmiş bir RSA anahtar oluşturma sistemi tavsiye etmişlerdir. Geliştirdikleri bu yeni sisteme ESRKGS adı verilmiştir. Tavsiye edilen bu algoritmada orijinal RSA'dan farklı olarak anahtar oluşturma aşamasında iki asal sayı değil de dört büyük asal sayıyı ele almışlardır. Uyguladıkları bu algoritmanın neticesine göre

görmüşlerdir ki önerdikleri modifiye edilen bu sistemin orijinal RSA'ya kıyasla daha çok güvenli ve üçüncü kişiler tarafından çabuk deşifre edilemeyeceğini ispatladıklarını söylemişlerdir.

2017 yılında Çavuşoğlu vd. , hibrit RSA (CRSA) Şifreleme Sistemi'ni oluşturmuşlardır. Bu algoritma RGN ve RSA şifreleme sistemlerinin bir arada kullanılmasıyla ortaya çıkan kaos tabanlı bir algoritmadır. Bu tasarımda metin ve görüntü şifreleme işleminin yapıldığından bahsetmişlerdir. Ayrıca algoritmanın güvenliğine yönelik yapılan analiz sonuçları ile orijinal RSA arasında yapılan karşılaştırılma ile varılan sonuç geliştirdikleri yeni şifreleme sisteminden elde edilen sonuçların daha iyi olduğudur.

2017 yılında El Makkaoui vd. , hızlı bulut-RSA'yı tasarlamışlardır. Bu tasarı ile bulut bilişimindeki verinin gizliliğinin korunması ve şifreli metni çözme aşamasındaki süreyi kısaltabilmeyi amaçlamışlardır. Sonuç olarak hızlı-RSA'nın işlem süresinde orijinal RSA'ya göre daha iyi bir sonuç elde edilmiştir. Böylece de işlem hızını artırırken aynı zamanda da istenilen güvenlik düzeyi sağlanmıştır.

2018 yılında Stergiou vd. , AES ve RSA şifreleme tekniklerinden faydalanarak IoT ve cloud teknolojilerinin uyum içinde çalışmasını sağlamışlardır. Şifreleme işlemlerinde RSA tekniğinin tercih edilmesiyle IoT'un işlevinde iletişim güvenliğinin daha fazla sağlanabileceği sonucuna ulaştıklarını söylemişlerdir.

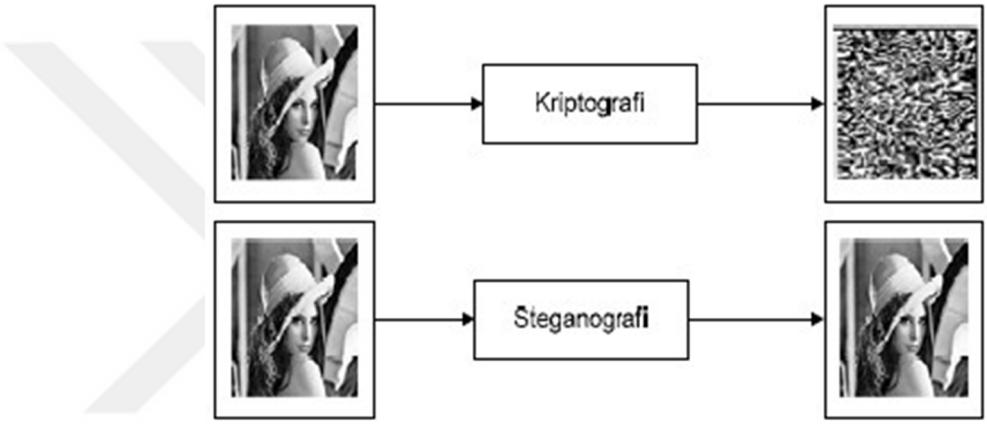
2018 yılında Liu vd. , RSA Şifreleme Metotu'ndan yararlanarak filigran modeli olarak bilinen daha güvenlikli ve sağlamlığı yüksek bir dijital görüntü şeması tavsiye etmişlerdir. Asimetrik şifreleme algoritmalarından biri olan RSA Algoritması'nı gizli verilerin güvenliğini garanti altına almak için kullanmışlardır. Yapmış oldukları deney sonuçlarına göre önerilen bu metodun benzer diğer tekniklere göre performans açısından değerlendirildiğinde daha sağlam, şifreleme hızı açısından bakıldığında yüksek hızlı ve büyük verileri saklama gücüne sahip olduğu görülmüştür.

2018 yılında Taha vd. , hybrit RSA şifreleme metodunu mobil bulut bilişim siteminde verinin güvenli şekilde korunmasını sağlayabilmek için tavsiye etmişlerdir.

2018 yılında Subhashini ve Srivaramangai tarafından yapılan bulut bilişim üzerine yaptıkları çalışma ile bulutta mevcut bilgilerin saklanıp korunmasının mümkün olmadığı durumda saklanmak ya da iletilmek istenen bilgilerin başkaları tarafından saldırıya uğramaya açık olduğunu ifade etmişlerdir. Bu sebeple bulut sistemde güvenliği yüksek seviyede tutabilmek adına yararlanılabilecek bir takım kriptografik

algoritmaların var olduğunu söylemişler ve bu algoritmaların modifiye edilmesi ile ilgili genel bir bakış sunarak tartışma başlatmışlardır.

2018 yılında Palathingal vd. , bulut sistemlerinde bilginin güvenli şekilde saklanıp veya iletilmesi için farklı bir yöntem uygulamışlardır. Steganografi adı verilen ve amacı üçüncü kişiler tarafından verileri gizlemek olan bu yöntemde sistemdeki verilerin güvenlik seviyesini yükseltebilmek için RSA Şifreleme Metodu ile diğer şifreleme metotlarını bir arada uyum içinde çalıştırarak bulut bilişim sisteminde daha kuvvetli bir sistem geliştirdiklerini göstermişlerdir [22].



Şekil 3. 2. Kriptografi ile steganografinin karşılaştırılmasını özetleyen resim

Burada sadece RSA ‘nın geçmişinden bahsetmekle kalınmamış aynı zamanda RSA’ nın başka metotlarla birlikte kullanımlarına ve bu metotlarla ayrı ayrı çalışıldığında ortaya çıkan sonuçlara ve bu metotlarla RSA’nın bazı özellikleri bakımından karşılaştırılmalarına değinilmiştir.

3.3. RSA Algoritmasının Kullanım Alanları

1. Askeri sistemler
2. Cep telefonları
3. Uzaktan kumandalar
4. Online bankacılık
5. Online alışveriş
6. Uydu alıcıları

7. Sim kartlar

Yukarıda bahsedildiği gibi uygulama alanı olan RSA Algoritması: Netscape Navigator ve Microsoft Internet Explorer web browser programlarının uygulamaları olan Secure Socket Layer (SSL) ve kredi kartı işlemleri için Secure Electronic Transaction (SET) protokolü ile Mastercard ve Vısa ayrıca S-HTTP, S/WAN, STT ve PCT uygulamalarında kullanılmaktadır [18]. Ayrıca S/MIME, PEM, MOSS ve PGP gibi gizli haberleşme protokolleri temel olarak RSA kullanır [31]. Ayrıca RSA Şifreleme Algoritması metinleri şifreleyerek başkası tarafından okunmaz hale getirmenin yanı sıra dijital ortamda verilerin imzalanması için de kullanılan algoritmadır Günümüzde de RSA Şifreleme Algoritması hala güvenilirliğini korumaktadır. Bunun nedeni modüler matematik üstüne kurulmuş, kripto analizi asal sayılara, çarpanlara ayırmaya dayalı anlaşılması kolay ama çözülmesi zor bir algoritma olmasıdır [25]. Bu algoritma aşağıda ifade edildiği gibidir:

3.4. RSA nın Genel Yapısı

3.4.1 Anahtar Üretimi

RSA da anahtar seçimi çok önemlidir. Çünkü şifreleme işlemini gerçekleştirecek olan anahtarın yeterince büyük ve uygun seçilmesi algoritmanın güvenilirliğini artıracaktır. Bu anahtar bir sayıdır. Bu anahtarı büyük seçmek dediğimiz gibi güvenilirliği artıracakken küçük seçmekte zamandan tasarrufu sağlayacaktır. Ancak şifreyi çözmek isteyen kişilerin saldırılarına da daha çok maruz kalacaktır. Anahtarın küçük seçilmesiyle bu saldırganlar bir takım saldırı metotlarıyla anahtarı ele geçirebilecek ve bu sayede şifreli metni deşifre edebilecektir. Seçilen anahtar kriptografik bir algoritma ile işler. Şimdi bu duruma göre anahtar oluşumuna bir göz atalım.

1. Birbirinden farklı p ve q asal sayıları seçilir.

2. $n = p.q$ değeri hesaplanır.

3. φ: Euler phi fonksiyonu olmak üzere;

$\varphi(n) = \varphi(p).\varphi(q) = (p-1).(q-1)$ totient değeri hesaplanır. İsveçli matematikçi Leonhard Euler tarafından bulunan ve Euler Totient diye ifade edilen Totient Fonsiyonu bir tam sayının kendisi ile aralarında asal ve bu sayıdan daha küçük olan sayı miktarının bulunduğu fonksiyon türüdür.

4. 1'den büyük $\varphi(n)$'den küçük $\varphi(n)$ ile aralarında asal bir *e* tamsayısı seçilir. Yani $1 < e < \varphi(n)$ ve $ebob(e, \varphi(n)) = 1$olacak şekilde bir *e* tamsayısı seçilir.

5. Seçilen *e* tamsayısının($mod\ \varphi(n)$) de tersi alınır ve *d* sonucu elde edilir yani $d \equiv e^{-1} mod(\varphi(n))$ değeri hesaplanır. Bu hesaplama Genişletilmiş Euclid Algoritması yardımı ile yapılır. Burada *d* sayısı *e*'nin *mod* ($\varphi(n)$)' e göre çarpımsal tersidir.

6. Böylece açık anahtar (*n,e*) ve gizli anahtarda (*n,d*) değeri olur [17].

Burada şifreleme ve deşifreleme anahtarlarının nasıl elde edileceği gösterilmiştir. Burada *n* halka açık olan anahtardır. Yani mesajın göndericisi de alıcısı da *n* değerinin ne olduğunu bilir. Ancak öte yandan *e* değerinin mesajın göndericisinin bilmesine rağmen *d* değerini sadece alıcı bilir. Bu da demektir ki *d* sadece alıcısının bildiği gizli anahtardır. *d* gizli anahtarın ele geçirilmesi demek mesajın çözülmesi demektir. Bununla beraber anahtar oluşturma sırasında aşağıda bahsi geçen uç problemin çözülme gerekliliği ortaya çıkmaktadır. Bu problemler;

- p ve q değerlerinin güvenlik açısından çok büyük asal sayılar olarak tercih edilmesi,
- $\varphi(n)$ ile aralarında asal olan başka deyişle $ebob(\varphi(n), d) = 1$ olan bir *d* değerinin bulunması,
- d'nin $mod(\varphi(n))$'e göre çarpımsal tersi olan *e* değerinin bulunması,

problemleridir. Bu üç problem Rabin-Miller asallık testi ve mod işlemine göre bir sayının çarpımsal tersinin bulunması yöntemleri kullanılarak çözülebilir [10]. Asimetrik şifreleme sisteminin tercih edilebilir olması için, bazı özellikleri yerine getirmelidir:

1. $\forall m < n$ için $m^e\ ve\ C^d$ hesaplanabilmelidir.
2. Sadece *e* ve *n* çifti bilindiğinde, *d* hesaplanamaz olmalıdır.

RSA şifreleme yönteminde anahtar büyüklüğü şifrelemeyi yapan kişiye göre değişmektedir. Uzunluğu 512 bit ile 2048 bit arasında olabilen anahtarın büyük seçilmesi güvenilirliği artıracaktır [20]. Önemli olan bu anahtar seçilirken bazı noktaların göz ardı edilmemesidir. Örneğin şifrelenerek saklanacak olan verinin ne kadar önemli olduğu, bu metnin ne kadar süre zarfında saklanacağı veya olası saldırı ihtimalleridir. Bu tür ihtimallerin ihmal edilmesi güvenliğin risk altına girmesine sebep olur.

3.4.2. Şifreleme

M: şifrelenecek veri, $0 \leq m \leq n - 1$

C : şifreli veri,

E : şifreleme algoritması

D : şifre çözme algoritması olmak üzere;

1. $M \in Z_n$ şifrelenmek istenen bilgi olsun.

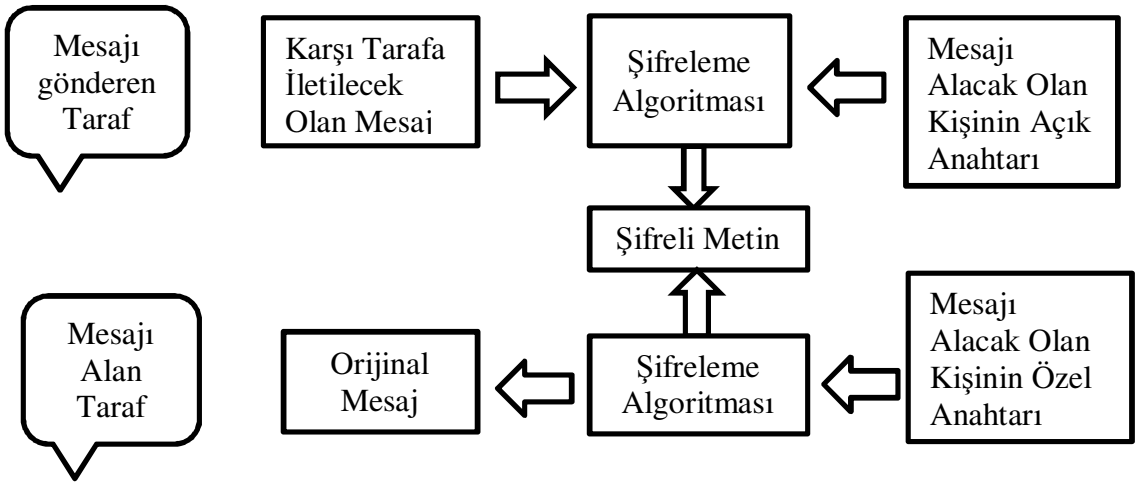
2. Şifrelenecek bu bilgi $[0, n-1]$ aralığında m sayısına dönüştürülür.

3. Şifre metni $C = E(m) = m^e (mod\ (n))$ olarak bulunur.

4. Bulunan C şifre metni karşı tarafa iletilir.

Şifreleme işlemi alıcısına ulaştırılmak üzere oluşturulan metnin veya mesajın, saldırganlar tarafından ele geçirilmesinin istenmediği zamanlarda uygulanan bir yöntemdir. Şifreleme için sistem herkeste olabilecek bir açık anahtara ve sadece alıcıda olacak gizli anahtara ihtiyaç duymaktadır. Seçilen iki büyük asal sayılara bir takım matematiksel algoritmalar uygulanmasıyla elde edilen bu anahtar çiftleri ile şifreleme işlemi gerçekleştirilir. Burada önemli olan açık bir ağ üzerinden iletilen bu bilgilerin, bahsi geçen üçüncü kişiler tarafından ya gizli anahtar ele geçirilerek ya da bir takım saldırı yöntemlerini kullanarak ele geçirilmesinin önlenmesidir. Bir şifreleme algoritmasının güvenlik açısından iyi bir algoritma olması demek o algoritmanın gizli anahtara ulaşamadan deşifre edilmesinin mümkün olmaması demektir.

C değeri hızlı üs alma yöntemi kullanılarak daha hızlı bir şekilde hesaplanır. Görüldüğü üzere şifreleme işlemi neticesinde oluşan C şifre metni de şifrelenecek veri olan m ile aynı aralıktadır. Şifreleme esnasında gönderici d anahtarını herkesten gizli tutarken (n,e) anahtar çiftini açık tutar, herkese yayınlar.



Şekil 3. 3. Şifrelenen bir mesajın gönderilmesi ve geri alınması

3.4.3 Deşifreleme

1. $D(C) = m \equiv C^d \ (mod\ n)$ değeri hesaplanır.

2. Daha sonra *m* tamsayıları ascıı kodlar kullanılarak *M* orijinal metine ulaşılır.

RSA Şifreleme Yöntemi'ni bu şekilde değil de tersinden düşündüğümüzde bu sefer şifreleme gizli anahtarla şifre çözme işlemi ise açık anahtar çiftiyle yapılır. İşlemi bu şekilde düşünmek demek mesaja kişinin sayısal imzasının atılması demektir. Ancak sayısal imzanın bütün metne uygulandığını düşünürsek bu baya zaman alıcıdır. O yüzden mesajın tamamını imzalamak yerine hash fonksiyonları tarafından oluşturulan ve 160 bit boyutunda olan mesajın özet kısmı imzalanır [8]. Bahsi geçen hash (özet) fonksiyonlarının bir takım özelliklerine değinecek olursak:

• Oluşturulan özetten yapılacak çıkarımla orijinal metne ulaşmak imkânsız olduğu için Hash fonksiyonlarının geriye dönüşü yoktur.

• Metnin özetine bakılarak birden fazla mesajı elde etmekte mümkün değildir. Bu da demektir ki her özet sadece bir mesaja aittir. Burada ki amaç ise her özeti bir mesaja ait kılarak mesajda yapılacak olan küçük bir değişikliğin sayısal imzayı geçersizleştirmesidir.

• Oluşturulan özet ele geçirildiği takdirde saldırganın ulaşacağı bilgiler anlamsızdır [17].

Örnek 3. 1

1. $p = 7 \quad q = 13$ olacak şekilde iki asal sayı seçilir.

2. $n = p.q$ değeri hesaplanır

$$n = 7.13 = 91$$

3. $\varphi(n) = (p-1)(q-1)$ Totient değeri bulunur.

$$\varphi(n) = (7-1)(13-1) = 6.12)72$$

4. $1 < e < \varphi(n) ve\ ebob\big(e, \varphi(n)\big) = 1$ olacak şekilde bir *e* tam sayısı seçilir.

$1 < e < 72\ ve\ ebob(e, 72) = 1$ olacak şekilde ki *e* sayısını *e=7* seçelim.

5. $d.e \equiv 1 mod\big(\varphi(n)\big)$ denkliğinden *d* değerini hesaplayalım.

$d.e \equiv 1mod(\varphi(n))$ ise $d.e = 1 + k.\varphi(n)$ $(k = 0,1,2, \dots \dots)$,

$d.7 = 1 + k.72$ $(k = 0,1,2, \dots \dots)$

genişletilmiş öklid algoritmasından faydalanarak *d* değerini bulalım.

$k = 0$ için $d.7 = 1 + 0.72$ den $d = \frac{1}{7}$ bunu seçemeyiz

$k = 1$ için $d.7 = 1 + 1.72$ den $d = \frac{73}{7}$ bunu seçemeyiz

$k = 2$ için $d.7 = 1 + 2.72$ den $d = \frac{145}{7}$ bunu seçemeyiz.

$k = 3$ için $d.7 = 1 + 3.72$ den $d = \frac{217}{7} = 31$ b□l□r□z.

6. Böylece açık anahtar (7,91) ve gizli anahtarda (31,91) olarak elde edilir.

Şimdi gelelim şifreleme işlemine:

Şifrelenecek mesaj $m = 8$ olsun.

$C \equiv m^e mod(\varphi(n))$ buna göre,

$C \equiv 8^7 mod(91)$

$8^1 \equiv 8mod(91)$

$8^2 \equiv 64mod(91)$

$8^3 \equiv 57mod(91)$

$8^4 \equiv 1mod(91)$

$C \equiv 8^7 mod(91) \equiv 8^3 8^4 mod(91) \equiv 57.1mod(91)$ dir.

Gelelim şifrelenmiş olan bu *m* mesajının deşifrelenmesine:

$D \equiv C^d mod(n)$ olduğunu biliyoruz.

$D \equiv 57^{31} mod(91)$

$57^1 \equiv 57mod(91)$

$57^2 \equiv 64 mod(91)$

$57^3 \equiv 8 mod(91)$

$57^4 \equiv 1 mod(91)$

$(57^4)^7 = 57^{28} \equiv 1 mod(91)$

$D \equiv 57^{31} mod(91) \equiv 57^{28} 57^3 mod(91) \equiv 1.8 mod(91)$ elde edilir.

Buradan da *D=8* yani orijinal mesaj bulunur.

Örnek 3. 2.

1. $p = 11$ $q = 19$ $olsun.$

2. $n = p.q = 11.19 = 209.$

3. $\varphi(n) = (p-1).(q-1) = (11-1).(19-1) = 180.$

4. $1 < e < \varphi(n)$ ve $ebob(e, \varphi(n)) = 1$ olacak şekilde *e* tamsayısını seçmeliyiz.

$1 < e < 180$ ve $ebob(e, 180) = 1$ olacak şekilde $e = 13$ olsun.

5. $d.e \equiv 1 mod(\varphi(n))$ olduğunu söylemiştik

$d.13 \equiv 1 mod(180)$ ise $d.13 = 1 + k.180$ (k=0,1,2……),

$k = 0$ için $d.13 = 1 + 0.180$ $d = \frac{1}{13}$ olur ki bunu seçemeyiz.

$k = 1$ için $d.13 = 1 + 1.180 = 181/13$ bunu seçemeyiz.

$k = 2$ için $d.13 = 1 + 2.180 = 361/13$ bunu seçemeyiz.

$k = 3$ için $d.13 = 1 + 3.180 = 541/13$ bunu seçemeyiz.

$k = 4$ için $d.13 = 1 + 4.180 = 721/13$ bunu seçemeyiz.

$k = 5$ için $d.13 = 1 + 5.180 = 901/13$ bunu seçemeyiz.

$k = 6$ için $d.13 = 1 + 6.180 = 1081/13$ bunu seçemeyiz.

$k = 7$ için $d.13 = 1 + 7.180 = 1261/13 = 97$ yani *d=97* dir.

Şifreleme işlemine gelelim. Şifrelenecek mesaj *m=57* olsun.

$C \equiv m^e mod(n) \equiv 57^{13} mod(209)$

$57^1 \equiv 57 mod(209)$

$57^2 \equiv 114 mod(209)$

$57^3 \equiv 19 mod(209)$

$57^5 = 57^{3+2} = 57^3 . 57^2 \equiv 19.114 mod(209) \equiv 76 mod(209)$

$57^8 = 57^{3+5} = 57^3 . 57^5 \equiv 19.76 mod(209) \equiv 190 mod(209)$

$57^{13} = 57^{5+8} = 57^5 . 57^8 \equiv 76.190 mod(209) \equiv 19 mod(209)$ dur.

Böylece şifreli mesaj *C=19* olarak elde edilmiş olur. Gelelim şifre çözme işlemine;

$D \equiv C^d mod(209) \equiv 19^{97} mod(209)$

$19^1 \equiv 19 mod(209)$

$19^2 \equiv 152 mod(209)$

$19^3 \equiv 171 mod(209)$

$19^4 \equiv 114 mod(209)$

$19^5 \equiv 76 mod(209)$

$19^6 \equiv 190 mod(209)$

$19^7 \equiv 57 mod(209)$

$19^8 \equiv 38 mod(209)$

$19^9 \equiv 95 mod(209)$

$19^{10} \equiv 133 mod(209)$

$19^{11} \equiv 19 mod(209)$

$19^{97} = 19^7 . (19^{10})^9 \equiv 57.133 mod(209) \equiv 57 mod(209)$ dur.

Görüldüğü üzere bu işlemlerle de orijinal mesaj *m=57* bulunmuş oldu.

Örnek 3. 3.

1. *p=11* ve *q=31*,

2. $p.q = 341$,

3. $(p-1).(q-1) = 300$,

4. $1 < e < 340$ ve $ebob(e, 300) = 1$ olacak şekilde $'$e yi 13 seçelim.

5. $d.13 = 1 + k.300 \quad (k = 0,1,2, \dots \dots)$,

$k = 0$ için $d = \frac{1}{13}$

$k = 1$ için $d = \frac{301}{13}$

$k = 2$ için $d = \frac{601}{13}$

$k = 3$ için $d = \frac{901}{13}$

$k = 4$ için $d = \frac{1201}{13}$

$\vdots$

$k = 12$ için $d = \frac{3601}{13} = 277$

$d = 277$ olarak seçebiliriz. Buna göre açık anahtar (*13, 341*) gizli anahtar (*277, 341*) olarak elde edilir.

Ali Ayşe'ye "ruveyda" kelimesini şifreleyerek gönderecek olsun. Önce bu mesajın ASCII tablosuna göre sayısal karşılıklarını bulmamız gerekir.

r	u	v	e	y	d	a
↓	↓	↓	↓	↓	↓	↓
114	117	118	101	121	100	97

$114^1 \equiv 114 mod(341)$

$114^2 \equiv 38 mod(341)$

$114^3 \equiv 240 mod(341)$

$114^{13} = (114^3)^4 . 114^1 \equiv 53 mod(341)$

$117^1 \equiv 117 mod(341)$

$117^2 \equiv 49 mod(341)$

$117^3 \equiv 277\ mod(341)$

$117^{13} = (117^3)^4 . 117^1 \equiv 167\ mod(341)$

$118^1 \equiv 118 mod(341)$

$118^2 \equiv 284 mod(341)$

$118^3 \equiv 94 mod(341)$

$118^{13} = (118^3)^4 . 118^1 \equiv 149 mod(341)$

$101^1 \equiv 101 mod(341)$

$101^2 \equiv 312 mod(341)$

$101^3 \equiv 48 mod(341)$

$101^{13} = (101^3)^4 . 101^1 \equiv 149 mod(341)$

$121^1 \equiv 121 mod(341)$

$121^2 \equiv 319 mod(341)$

$121^3 \equiv 66 mod(341)$

$121^{13} = (121^3)^4 . 121^1 \equiv 286 mod(341)$

$100^1 \equiv 100 mod(341)$

$100^2 \equiv 111 mod(341)$

$100^3 \equiv 188 mod(341)$

$100^{13} = (100^3)^4 . 100^1 \equiv 298 mod(341)$

$97^1 \equiv 97 mod(341)$

$97^2 \equiv 202 mod(341)$

$97^3 \equiv 157 mod(341)$

$97^{13} = (97^3)^4 . 97^1 \equiv 157 mod(341)$

$D \equiv C^{277} mod(341)$

$53^1 \equiv 53 mod(341)$

$53^2 \equiv 81 mod(341)$

$53^4 = 53^2 . 53^2 \equiv (81.81) mod(341) \equiv 82 mod(341)$

$53^8 = 53^4 . 53^4 \equiv (82.82) mod(341) \equiv 245 mod(341)$

$53^{16} = 53^8 . 53^8 \equiv (245.245) mod(341) \equiv 9 mod(341)$

$53^{32} = 53^{16} . 53^{16} \equiv (9.9) mod(341) \equiv 81 mod(341)$

$53^{277} = (53^{30})^9 . (53^2)^3 . 53^1 \equiv 114 mod(341)$

$167^1 \equiv 167 mod(341)$

$167^2 \equiv 268 mod(341)$

$167^4 = 167^2 . 167^2 \equiv (268.268) mod(341) \equiv 214 mod(341)$

$167^8 = 167^4 . 167^4 \equiv (214.214) mod(341) \equiv 102 mod(341)$

$167^{16} = 167^8 . 167^8 \equiv (102.102) mod(341) \equiv 174 mod(341)$

$167^{32} = 167^{16} . 167^{16} \equiv (174.174) mod(341) \equiv 268 mod(341)$

$167^{277} = (167^{30})^9 . (167^2)^3 . 167^1 \equiv 117 mod(341)$

$149^1 \equiv 149 mod(341)$

$149^2 \equiv 36 mod(341)$

$149^4 = 149^2.149^2 \equiv (36.36) mod(341) \equiv 273 mod(341)$

$149^8 = 149^4.149^4 \equiv (273.273) mod(341) \equiv 191 mod(341)$

$149^{16} = 149^8.149^8 \equiv (191.191) mod(341) \equiv 335 mod(341)$

$149^{32} = 149^{16}.149^{16} \equiv (335.335) mod(341) \equiv 36 mod(341)$

$149^{277} = (149^{30})^9.(149^2)^3.149^1 \equiv 118 mod(341)$

$286^1 \equiv 286 mod(341)$

$286^2 \equiv 297 mod(341)$

$286^4 = 286^2.286^2 \equiv (297.297) mod(341) \equiv 231 mod(341)$

$286^8 = 286^4.286^4 \equiv (231.231) mod(341) \equiv 165 mod(341)$

$286^{16} = 286^8.286^8 \equiv (165.165) mod(341) \equiv 286 mod(341)$

$286^{32} = 286^{16}.286^{16} \equiv (286.286) mod(341) \equiv 297 mod(341)$

$286^{277} = (286^{30})^9.(286^2)^3.286^1 \equiv 121 mod(341)$

$298^1 \equiv 298 mod(341)$

$298^2 \equiv 144 mod(341)$

$298^4 = 298^2.298^2 \equiv (144.144) mod(341) \equiv 276 mod(341)$

$298^8 = 298^4.298^4 \equiv (276.276) mod(341) \equiv 133 mod(341)$

$298^{16} = 298^8.298^8 \equiv (133.133) mod(341) \equiv 298 mod(341)$

$298^{277} \equiv 100 mod(341)$

$157^1 \equiv 157 mod(341)$

$157^2 \equiv 97 mod(341)$

$157^4 = 157^2.157^2 \equiv (97.97) mod(341) \equiv 202 mod(341)$

$157^8 = 157^4.157^4 \equiv (202.202) mod(341) \equiv 225 mod(341)$

$157^{16} = 157^8.157^8 \equiv (225.225) mod(341) \equiv 157 mod(341)$

$157^{277} \equiv 97 mod(341)$ dir.

Örnek 3. 4.

1. $p = 7$ $q = 17$ $olsun.$

2. $n = 7.17 = 119$

3. $\varphi(n) = (7-1)(17-1) = 96$

4. $1 < e < 96$ ve $ebob(e, 96) = 1$ olacak şekilde e tamsayısını $e = 5$ seçelim.

5. $d.e \equiv 1 mod\big(\varphi(n)\big)$ den,

$d.e = 1 + k.96 \qquad (k = 0,1,2, \dots \dots),$

$k = 0$ için $d.5 = 1 + 0.96$ dan $d = 1/5$

$k = 1$ için $d.5 = 1 + 1.96$ dan $d = \frac{97}{5}$

$k = 2$ için $d.5 = 1 + 2.96$ dan $d = 193/5$

$k = 3$ için $d.e = 1 + 3.96$ dan $d = 289/5$

$k = 4$ için $d.5 = 1 + 4.96$ dan $d = \frac{385}{5} = 77$

$d = 77$ olarak elde ettik. Şimdi gelelim şifreleme işlemine:

Şifreleyeceğimiz metin “ali gel” olsun. Bu metnin sayısal karşılığı:

a	l	i	g	e	l
↓	↓	↓	↓	↓	↓
97	108	105	103	101	108

$C \equiv m^e mod\ (n) \equiv m^5 mod(119)$

$C \equiv 97^5 108^5 105^5 103^5 101^5 108^5 mod(119)$

$97^1 \equiv 97 mod(119)$

$97^2 \equiv 8 mod(119)$

$97^3 \equiv 62 mod(119)$

$97^5 = 97^3 . 97^2 \equiv (62.8) mod(119) \equiv 20 mod(119)$

$108^1 \equiv 108 mod(119)$

$108^2 \equiv 2 mod(119)$

$108^3 \equiv 97 mod(119)$

$108^5 = 108^3 . 108^2 \equiv (97.2) mod(119) \equiv 75 mod(119)$

$105^1 \equiv 105 mod(119)$

$105^2 \equiv 77 mod(119)$

$105^3 \equiv 112 mod(119)$

$105^5 = 105^3 . 105^2 \equiv (112.77) mod(119) \equiv 56 mod(119)$

$103^1 \equiv 103 mod(119)$

$103^2 \equiv 18 mod(119)$

$103^3 \equiv 69 mod(119)$

$103^5 = 103^3 . 103^2 \equiv (69.18) mod(119) \equiv 52 mod(119)$

$101^1 \equiv 101 mod(119)$

$101^2 \equiv 86\, mod(119)$

$101^3 \equiv 118 mod(119)$

$101^5 = 101^3 . 101^2 \equiv (118.86) mod(119) \equiv 33 mod(119)$ dur.

Yapılan bu işlemlere göre şifrelenmiş metnimiz

20 75 56 52 33 75

olur. Şimdi şifrelenmiş bu metni deşifreleyelim.

$$D \equiv C^d mod(n) \text{ den } D \equiv C^{77} mod(119)$$

denkliğini hesaplayacağız.

$20^1 \equiv 20 mod(119)$

$20^2 \equiv 43 mod(119)$

$20^3 \equiv 27 mod(119)$

$20^5 \equiv 90 mod(119)$

$20^{10} = 20^5 . 20^5 \equiv (90.90) mod(119) \equiv 8 mod(119)$

$20^{20} = 20^{10} . 20^{10} \equiv (8.8) mod(119) \equiv 64 mod(119)$

$20^{40} = 20^{20} . 20^{20} \equiv (64.64) mod(119) \equiv 50 mod(119)$

$20^{77} = 20^{40} 20^{20} 20^{10} 20^5 20^2 \equiv (50.64.8.90.43) mod(119) \equiv 97 mod(119)$

$75^1 \equiv 75 mod(119)$

$75^2 \equiv 32 mod(119)$

$75^3 \equiv 20 mod(119)$

$75^5 = 75^3 . 75^2 \equiv (20.32) mod(119) \equiv 45 mod(119)$

$75^{10} = 75^5 . 75^5 \equiv (45.45) mod(119) \equiv 2 mod(119)$

$75^{20} = 75^{10} . 75^{10} \equiv (2.2) mod(119) \equiv 4 mod(119)$

$75^{40} = 75^{20} . 75^{20} \equiv (4.4) mod(119) \equiv 16 mod(119)$

$75^{77} = 75^{40} . 75^{20} . 75^{10} . 75^5 . 75^2 \equiv (16.4.2.45.32) mod(119) \equiv 108 mod(119)$

$56^1 \equiv 56 mod(119)$

$56^2 \equiv 42 mod(119)$

$56^3 \equiv 91 mod(119)$

$56^5 = 56^3.56^2 \equiv (91.42) mod(119) \equiv 14 mod(119)$

$56^6 = 56^3.56^3 \equiv (91.91) mod(119) \equiv 70 mod(119)$

$56^{12} = 56^6.56^6 \equiv 70.70 mod(119) \equiv 21 mod(119)$

$56^{24} = 56^{12}.56^{12} \equiv (21.21) mod(119) \equiv 84 mod(119)$

$56^{48} = 56^{24}.56^{24} \equiv (84.84) mod(119) \equiv 35 mod(119)$

$56^{77} = 56^{48}.56^{24}.56^5 \equiv (35.84.14) mod(119) \equiv 105 mod(119)$

$52^1 \equiv 52 mod(119)$

$52^2 \equiv 86 mod(119)$

$52^3 \equiv 69 mod(119)$

$52^5 = 52^3.52^2 \equiv 103 mod(119)$

$52^{10} = 52^5.52^5 \equiv (103.103)\ mod(119) \equiv 18 mod(119)$

$52^{20} = 52^{10}.52^{10} \equiv (18.18) mod(119) \equiv 86 mod(119)$

$52^{40} = 52^{20}.52^{20} \equiv (86.86) mod(119) \equiv 18 mod(119)$

$52^{77} = 52^{40}.52^{20}.52^{10}.52^5.52^2 \equiv (18.86.18.103.86)\ mod(119) \equiv 103 mod(119)$

$33^1 \equiv 33 mod(119)$

$33^2 \equiv 18 mod(119)$

$33^3 \equiv 118 mod(119)$

$33^5 = 33^3.33^2 \equiv (118.18) mod(119) \equiv 101 mod(119)$

$33^{10} = 33^5.33^5 \equiv (101.101) mod(119) \equiv 86 mod(119)$

$33^{20} = 33^{10}.33^{10} \equiv (86.86) mod(119) \equiv 18 mod(119)$

$33^{40} = 33^{20}.33^{20} \equiv (18.18) mod(119) \equiv 86 mod(119)$

$33^{77} = 33^{40}.33^{20}.33^{10}.33^{5}.33^{2} \equiv (86.18.86.101.18) mod(119) \equiv 101 mod(119)$ elde edilir.

Örnek 3. 5.

1. $p = 23$ $q = 19$ olsun.

2. $n = p.q = 23.19 = 437$,

3. $\varphi(n) = 22.18 = 396$,

4. $1 < e < 396$ ve $ebob(e, 396) = 1$ olacak şekilde $e = 7$ olsun.

5. $d.e = 1 + k.\varphi(n)$ $(k = 0,1,2, \dots \dots)$,

$k = 0$ için d=1/7

$k = 1$ için $d.7 = 1 + 1.396$ dan $d = \frac{397}{7}$

$k = 2$ için $d.7 = 1 + 2.396$ dan $d = \frac{793}{7}$

$k = 5$ için $d.7 = 1 + 5.396$ dan $d = \frac{1981}{7} = 283$

$d = 283$ olarak elde ettik.

Şifrelenecek metnimiz, “bu mesaj bir hayli gizlidir” olsun. Bu metnin sayısal karşılığı:

b	u	m	e	s	a	j	b	i	r
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
98	117	109	101	115	97	106	98	105	114

h	a	y	l	i	g	i	z	l	i	d	i	r
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
104	97	121	108	105	103	105	122	108	105	100	105	114

dir. Şimdi gerekli şifreleme işlemlerini yapacak olursak;

$98^1 \equiv 98 mod(437)$

$98^2 \equiv 427 mod(437)$

$98^3 \equiv 331 mod(437)$

$98^5 = 98^3 . 98^2 \equiv (331.427) mod(437) \equiv 186 mod(437)$

$98^7 = 98^5 . 98^2 \equiv (186.427) mod(437) \equiv 325 mod(437)$

$117^1 \equiv 117 mod(437)$

$117^2 \equiv 142 mod(437)$

$117^3 \equiv 8 mod(437)$

$117^5 = 117^3 . 117^2 \equiv (8.142) mod(437) \equiv 262 mod(437)$

$117^7 = 117^5 . 117^2 \equiv (262.142) mod(437) \equiv 59 mod(437)$

$109^1 \equiv 109 mod(437)$

$109^2 \equiv 82 mod(437)$

$109^3 \equiv 198 mod(437)$

$109^5 = 109^3 . 109^2 \equiv (198.82) mod(437) \equiv 67 mod(437)$

$109^7 = 109^5 . 109^2 \equiv (67.82) mod(437) \equiv 250 mod(437)$

$101^1 \equiv 101 mod(437)$

$101^2 \equiv 150 mod(437)$

$101^3 \equiv 292 mod(437)$

$101^5 = 101^3 . 101^2 \equiv (292.150) mod(437) \equiv 100 mod(437)$

$101^7 = 101^5 . 101^2 \equiv (100.150) mod(437) \equiv 142 mod(437)$

$115^1 \equiv 115 mod(437)$

$115^2 \equiv 115 mod(437)$

$115^7 \equiv 115 mod(437)$

$97^1 \equiv 97 mod(437)$

$97^2 \equiv 232 mod(437)$

$97^3 \equiv 217 mod(437)$

$97^5 = 97^3 . 97^2 \equiv (217.232) mod(437) \equiv 89 mod(437)$

$97^7 = 97^5 . 97^2 \equiv (89.232) mod(437) \equiv 109 mod(437)$

$106^1 \equiv 106 mod(437)$

$106^2 \equiv 311 mod(437)$

$106^3 \equiv 191 mod(437)$

$106^5 = 106^3 . 106^2 \equiv (311.191) mod(437) \equiv 406 mod(437)$

$106^7 = 106^5 . 106^2 \equiv (406.311) mod(437) \equiv 410 mod(437)$

$105^1 \equiv 105 mod(437)$

$105^2 \equiv 100 mod(437)$

$105^3 \equiv 12 mod(437)$

$105^5 = 105^3 . 105^2 \equiv (12.100) mod(437) \equiv 326 mod(437)$

$105^7 = 105^5 . 105^2 \equiv (201.100) mod(437) \equiv 262 mod(437)$

$114^1 \equiv 114 mod(437)$

$114^2 \equiv 323 mod(437)$

$114^3 \equiv 114 mod(437)$

$114^7 \equiv 114 mod(437)$

$104^1 \equiv 104 mod(437)$

$104^2 \equiv 328 mod(437)$

$104^3 \equiv 26 mod(437)$

$104^5 = 104^3.104^2 \equiv (26.328) mod(437) \equiv 225 mod(437)$

$104^7 = 104^5.104^2 \equiv (225.328) mod(437) \equiv 384 mod(437)$

$121^1 \equiv 121 mod(437)$

$121^2 \equiv 220 mod(437)$

$121^3 \equiv 400 mod(437)$

$121^5 = 121^3.121^2 \equiv (400.220) mod(437) \equiv 163 mod(437)$

$121^7 = 121^5.121^2 \equiv (163.220) mod(437) \equiv 26 mod(437)$

$108^1 \equiv 108\, mod(437)$

$108^2 \equiv 302 mod(437)$

$108^3 \equiv 278 mod(437)$

$108^5 = 108^3.108^2 \equiv (278.302) mod(437) \equiv 52 mod(437)$

$108^7 = 105^5.108^2 \equiv (52.302) mod(437) \equiv 409 mod(437)$

$103^1 \equiv 103 mod(437)$

$103^2 \equiv 121 mod(437)$

$103^3 \equiv 227 mod(437)$

$103^5 = 103^3.103^2 \equiv (227.121) mod(437) \equiv 373 mod(437)$

$103^7 = 103^5.103^2 \equiv (373.121) mod(437) \equiv 122 mod(437)$

$122^1 \equiv 122 mod(437)$

$122^2 \equiv 26 mod(437)$

$122^3 \equiv 113 mod(437)$

$122^5 = 122^3.122^2 \equiv (113.26)mod(437) \equiv 316mod(437)$

$122^7 = 122^5.122^2 \equiv (316.26)mod(437) \equiv 350mod(437)$

$100^1 \equiv 100mod(437)$

$100^2 \equiv 386\ mod(437)$

$100^3 \equiv 144mod(437)$

$100^5 = 100^3.100^2 \equiv (144.386)mod(437) \equiv 85mod(437)$

$100^7 = 100^5.100^2 \equiv (85.386)mod(437) \equiv 35mod(437)$ dir.

Metnin şifreli hali

325 59 250 142 115 109 410 325 262 114 384 109 26 409 262 122 262 350 409 262 35 262 114 dür.

Gelelim deşifreleme işlemine.

$D \equiv C^{283}mod(437)$

$325^1 \equiv 325mod(437)$

$325^2 \equiv 308mod(437)$

$325^3 \equiv 27mod(437)$

$325^4 \equiv 35mod(437)$

$325^8 = 325^4.325^4 \equiv (35.35)mod(437) \equiv 351mod(437)$

$328^{16} = 325^8.328^8 \equiv (351.351)mod(437) \equiv 404\ mod(437)$

$325^{32} = 325^{16}.325^{16} \equiv (404.404)mod(437) \equiv 215mod(437)$

$325^{283} = (325^{32})^8.325^{16}.325^8.325^3 \equiv (73.404.351.27)mod(437) \equiv$

$98mod(437)$

$59^1 \equiv 59mod(437)$

$59^2 \equiv 422 mod(437)$

$59^3 \equiv 426 mod(437)$

$59^4 \equiv 225 mod(437)$

$59^8 \equiv 59^4 . 59^4 \equiv (225.225) mod(437) \equiv 370 mod(437)$

$59^{16} = 59^8 . 59^8 \equiv (370.370) mod(437) \equiv 119 mod(437)$

$59^{32} = 59^{16} . 59^{16} \equiv (119.119) mod(437) \equiv 177 mod(437)$

$59^{283} = (59^{32})^8 . 59^{16} . 59^8 . 59^3 \equiv (35.119.370.426) mod(437) \equiv 117 mod(437)$

$250^1 \equiv 250 mod(437)$

$250^2 \equiv 9 mod(437)$

$250^3 \equiv 65 mod(437)$

$250^4 \equiv 81 mod(437)$

$250^8 = 250^4 . 250^4 \equiv (81.81) mod(437) \equiv 6 mod(437)$

$250^{16} = 250^8 . 250^8 \equiv (6.6) mod(437) \equiv 36 mod(437)$

$250^{32} = 250^{16} . 250^{16} \equiv (36.36) mod(437) \equiv 422 mod(437)$

$250^{283} = (250^{32})^8 . 250^{16} . 250^8 . 250^3 \equiv (119.36.6.65) mod(437) \equiv 109 mod(437)$

$142^1 \equiv 142 mod(437)$

$142^2 \equiv 62 mod(437)$

$142^3 \equiv 64$

$142^4 = 142^2 . 142^2 \equiv (62.62) mod(437) \equiv 348 mod(437)$

$142^8 = 142^4 . 142^4 \equiv (348.348) mod(437) \equiv 55 mod(437)$

$142^{16} = 142^8 . 142^8 \equiv (55.55) mod(437) \equiv 403 mod(437)$

$142^{32} = 142^{16} . 142^{16} \equiv (403.403) mod(437) \equiv 282 mod(437)$

$142^{283} = (142^{32})^{8}.142^{16}.142^{8}.142^{3} \equiv (386.403.55.64)mod(437) \equiv 101mod(437)$

$115^{283} \equiv 115mod(437)$

$109^{1} \equiv 109\ mod(437)$

$109^{2} \equiv 82mod(437)$

$109^{3} \equiv 198mod(437)$

$109^{4} = 109^{2}.109^{2} \equiv (82.82)mod(437) \equiv 169mod(437)$

$109^{8} = 109^{4}.109^{4} \equiv (169.169)mod(437) \equiv 156mod(437)$

$109^{16} = 109^{8}.109^{8} \equiv (156.156)mod(437) \equiv 301mod(437)$

$109^{32} = 109^{8}.109^{8} \equiv (301.301)mod(437) \equiv 142mod(437)$

$109^{283} = (109^{32})^{8}.109^{16}.109^{8}.109^{3} \equiv (55.301.156.198)mod(437) \equiv 97mod(437)$

$410^{1} \equiv 410mod(437)$

$410^{2} \equiv 292mod(437)$

$410^{3} \equiv 419mod(437)$

$410^{4} = 410^{2}.410^{2} \equiv (292.292)mod(437) \equiv 49mod(437)$

$410^{8} = 410^{4}.410^{4} \equiv (49.49)mod(437) \equiv 216mod(437)$

$410^{16} = 410^{8}.410^{8} = (216.216)mod(437) \equiv 334mod(437)$

$410^{32} = 410^{16}.410^{16} \equiv (334.334)\ mod(437) \equiv 121mod(437)$

$410^{283} = (410^{32})^{8}.410^{16}.410^{8}.410^{3} \equiv (87.334.216.419)mod(437) \equiv 106mod(437)$

$262^{1} \equiv 262mod(437)$

$262^{2} \equiv 35mod(437)$

$262^3 \equiv 430 mod(437)$

$262^4 = 262^2.262^2 \equiv (35.35) mod(437) \equiv 351 mod(437)$

$262^8 = 262^4.262^4 \equiv (351.351) mod(437) \equiv 404 mod(437)$

$262^{16} = 262^8.262^8 \equiv (404.404) mod(437) \equiv 215 mod(437)$

$262^{32} = 262^{16}.262^{16} \equiv (215.215) mod(437) \equiv 340 mod(437)$

$262^{283} = (262^{32})^8.262^{16}.262^8.262^3 \equiv (85.215.404.430) mod(437) \equiv 105 mod(437)$

$114^1 \equiv 114 mod(437)$

$114^2 \equiv 323 mod(437)$

$114^3 \equiv 114 mod(437)$

$114^{283} = (114^2)^{141}.114^1 \equiv (323.114) mod(437) \equiv 114 mod(437)$

$384^1 \equiv 384 mod(437)$

$384^2 \equiv 187 mod(437)$

$384^3 \equiv 140 mod(437)$

$384^4 = 384^2.384^2 \equiv (187.187) mod(437) \equiv 9 mod(437)$

$384^8 = 384^4.384^4 \equiv (9.9) mod(437) \equiv 81 mod(437)$

$384^{16} = 384^8.384^8 \equiv (81.81) mod(437) \equiv 6 mod(437)$

$384^{32} = 384^{16}.384^{16} \equiv (6.6) mod(437) \equiv 36 mod(437)$

$384^{283} = (384^{32})^8.384^{16}.384^8.384^3 \equiv (370.6.81.140) mod(437) \equiv 104 mod(437)$

$26^1 \equiv 26 mod(437)$

$26^2 \equiv 239 mod(437)$

$26^3 \equiv 96 mod(437)$

$26^4 = 26^2.26^2 \equiv (239.239)\ mod(437) \equiv 311 mod(437)$

$26^8 = 26^4.26^4 \equiv (311.311) mod(437) \equiv 144 mod(437)$

$26^{16} = 26^8.26^8 \equiv (144.144) mod(437) \equiv 197 mod(437)$

$26^{32} = 26^{16}.26^{16} \equiv (197.197) mod(437) \equiv 353 mod(437)$

$26^{283} = (26^{32})^8.26^{16}.26^8.26^3 \equiv (349.197.144.96) mod(437) \equiv 121 mod(437)$

$409^1 \equiv 409 mod(437)$

$409^2 \equiv 347 mod(437)$

$409^3 \equiv 335 mod(437)$

$409^4 = 409^2.409^2 \equiv (347.347) mod(437) \equiv 234 mod(437)$

$409^8 = 409^4.409^4 \equiv (234.234) mod(437) \equiv 131 mod(437)$

$409^{16} = 409^8.409^8 \equiv (131.131) mod(437) \equiv 118 mod(437)$

$409^{32} = 409^{16}.409^{16} \equiv (118.118) mod(437) \equiv 377 mod(437)$

$409^{283} = (409^{32})^8.409^{16}.409^8.409^3 \equiv (377.118.131.335) mod(437) \equiv 108 mod(437)$

$122^1 \equiv 122 mod(437)$

$122^2 \equiv 26 mod(437)$

$122^3 \equiv 113 mod(437)$

$122^4 = 122^2.122^2 \equiv (26.26) mod(437) \equiv 239 mod(437)$

$122^8 = 122^4.122^4 \equiv (239.239) mod(437) \equiv 311 mod(437)$

$122^{16} = 122^8.122^8 \equiv (311.311) mod(437) \equiv 144 mod(437)$

$122^{32} = 122^{16}.122^{16} \equiv (144.144) mod(437) \equiv 197 mod(437)$

$122^{283} = (122^{32})^8 . 122^{16} . 122^8 . 122^3 \equiv (163.144.311.113) mod(437) \equiv$

$103 mod(437)$

$350^1 \equiv 350 mod(437)$

$350^2 \equiv 140 mod(437)$

$350^3 \equiv 56 mod(437)$

$350^4 = 350^2 . 350^2 \equiv (140.140) mod(437) \equiv 372 mod(437)$

$350^8 = 350^4 . 350^4 \equiv (372.372) mod(437) \equiv 292 mod(437)$

$350^{16} = 350^8 . 350^8 \equiv (292.292) mod(437) \equiv 49 mod(437)$

$350^{32} = 350^{16} . 350^{16} \equiv (49.49) mod(437) \equiv 216 mod(437)$

$350^{283} = (350^{32})^8 . 350^{16} . 350^8 . 350^3 \equiv (220.49.292.56) mod(437) \equiv$

$122 mod(437)$

$35^1 \equiv 35 mod(437)$

$35^2 \equiv 351 mod(437)$

$35^3 \equiv 49 mod(437)$

$35^4 = 35^2 . 35^2 \equiv (351.351) mod(437) \equiv 404 mod(437)$

$35^8 = 35^4 . 35^4 \equiv (404.404) mod(437) \equiv 215 mod(437)$

$35^{16} = 35^8 . 35^8 \equiv (215.215) mod(437) \equiv 340 mod(437)$

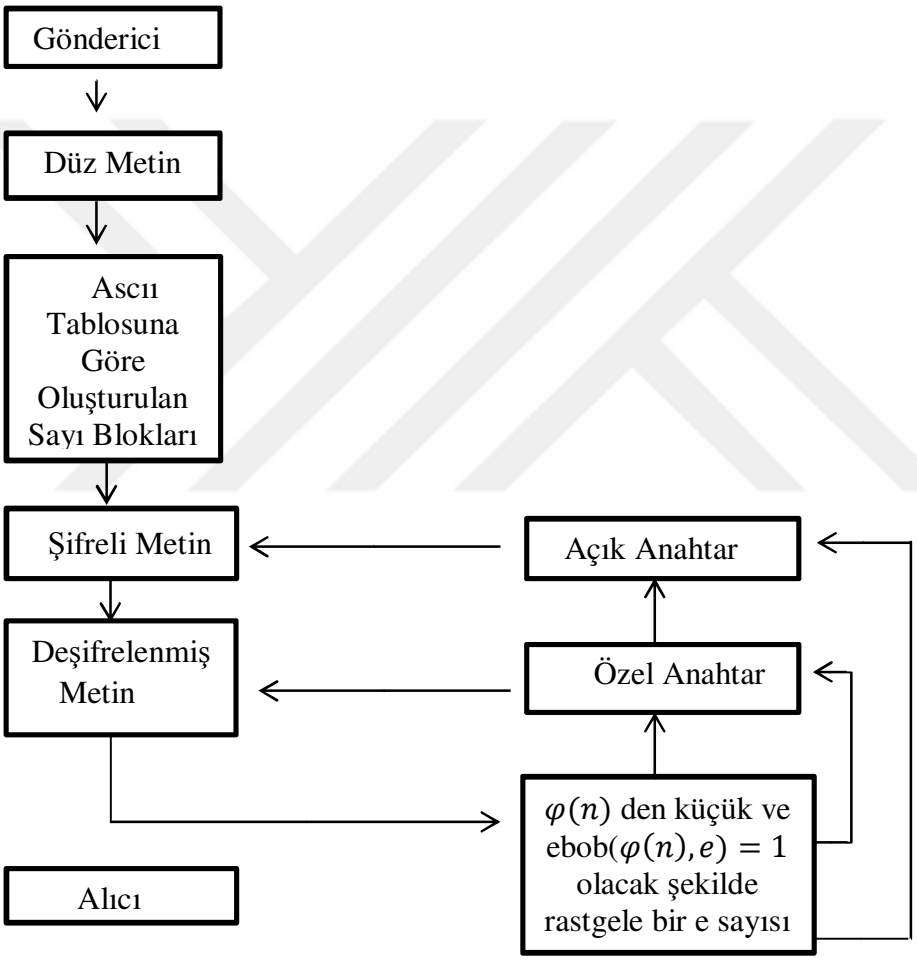
$35^{32} = 35^{16} . 35^{16} \equiv (340.340) mod(437) \equiv 232 mod(437)$

$35^{283} = (35^{32})^8 . 35^{16} . 35^8 . 35^3 \equiv (233.340.215.49) mod(437) \equiv 100 mod(437)$
dir.

RSA algoritmasında iki asal sayının çarpımını kullanarak anahtar oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmanın asal olmayan sayıları ayırmaktan daha zor olmasıdır. Böylece üretilen anahtarın elde edilmesi daha zor

olacaktır. Buda RSA' nın daha güvenli bir hal almasının sebebidir. Ayrıca bu algoritmada iki tamsayının aralarında asal olup olmadığını anlamak için matematikteki Öklid algoritmasından yararlanılır [31]. Bir şifreleme algoritması olarak RSA algoritması oldukça basit bir algoritmadır. Öteki taraftan da bu algoritmada sürekli çok büyük asal sayı oluşturmak oldukça zor bir işlemdir.

3.5. Rsa şifreleme metodunun genel işleyişi



Şekil 3. 4. RSA'nın genel işleyiş şeması [22]

Şekilden anlaşıldığı ve daha önce bahsettiğimiz gibi RSA Şifreleme Algoritması'nda en önemli şey, birbirinden farklı ve yeterince büyük iki asal sayının tercih edilmesidir. Seçilen asal sayılar aynı uzunlukta olmalı. Bu sayıların asal olup olmadığı da belirli asallık testleriyle tespit edilir. 2020 yılına kadar NIST tarafından belirlenen her bir asal sayının uzunluğu 1024 bittir. Uygun seçilen asal sayılar ile oluşturulan anahtara bir

sahip olduğu gizli anahtar sayesinde yine bu anahtara bir takım matematiksel algoritmalar uygulanarak deşifre edilir [8].

Tablo 3. 2. RSA şifreleme sistemine örnek [22]

RSA şifreleme metodu	Örnek
İlk adım olarak asal olan iki sayı seçilir	$p=11$ ve $q=7$ seçelim
$p.q$ deperi hesaplanır	$p.q = 11.7 = 77$
Totient değeri hesaplanır	$(p-1).(q-1) = (11-1)(7-1) = 60$
Bu Totient değeri ile aralarında asal olan ve $1 < e < \varphi(n)$ olacak şekilde e değeri bulunur	$1 < e < 60$ ve $ebob(e, 60) = 1$olacak şekilde $e = 17$ seçelim
$d.e = 1 mod(\varphi(n))$ ifadesinde d hesaplanır.	$d.17 = 1 mod 60$
Açık anahtar (e,n) olur	$(17,77)$ açık anahtar
Gizli anahtar (d,e) olur	$(d,77)$ gizli anahtar

3.6. RSA Algoritmasının Hızını Artıran İşlemler

i. Hızlı üs alma
ii. Açık anahtarın küçük seçilmesi
iii. Çin kalan teoremi
iv. Büyük asal sayı bulma

işlemleri RSA' nın hızını artırmaya yönelik işlemlerdir.

3.6.1. Hızlı Üs Alma

Seçilen sayılar büyüdükçe RSA Algoritması'nda işlem hızını artıracak bazı yöntemlere ihtiyaç duyulmuştur. Çarpma ve kare alma algoritması bu yöntemlere bir örnektir. Burada önemli olan herhangi bir b için $a^{b'}$nin $mod(c)$ ye göre denk olduğu ifadeyi bulabilmek için b' nin 2' nin bir kuvveti olup olmadığını belirlemektir.

Eğer b ikinin kuvveti ise:

$a^1, a^2, a^3, a^4, \ldots\ldots a^b$ İfadeleri modüler aritmetik kuralları kullanılarak ve her bulunan sonuç bir sonraki denklikte yerine konularak istenen sonuca ulaşılır. Bu işlem RSA' nın hızını artırmaya yönelik bir işlemdir [13].

3.6.2.Açık Anahtarın Küçük Seçilmesi

Açık anahtar *e'* yi 3,17 gibi küçük hamming ağırlığına sahip bir sayı olarak seçmenin amacı, çarpma ve kare alma işlem sayısını azaltarak RSA nın hızını artırmaktır [13].

3.6.3. Çinli Kalan Teoremi

RSA ya giriş yaparken bu algoritmada açık ve gizli olmak üzere iki anahtar kullanıldığından bahsetmiştik. RSA nın hızını artırmak için açık anahtar *e'* yi ne kadar küçük seçiyorsak bu durumun aksine gizli anahtarı da bir o kadar büyük seçmeliyiz. Bunun amacı gizli anahtarı büyük seçerek güvenliği artırıp olası RSA şifreleme algoritmasına karşı olabilecek saldırıların kaba kuvvet saldırısı) önlemektir. Ancak bu değerin büyük seçilmesi de RSA da deşifreleme ve sayısal imza işlemlerinin hız kazanması açısından yeni bir metoda gereksinim olmuştur. İşte bu noktada çinli kalan teoremi devreye girmiş ve bu yöntemle de işlemler hız kazanmıştır. Quisquater and Couvreur 1982 yılında CRT-RSA ismini verdikleri ve orijinal RSA ya göre dört kat daha fazla hıza sahip bir yapıyı bu yöntemle oluşturmuşlardır [13].

3.6.4. Büyük Asal Sayı Bulma

RSA Algoritması'nın anahtar üretme işleminde ilk adım *p* ve *q* olmak üzere güvenlik açısından tercih edilen büyüklükte iki asal sayıyı seçmek olduğunu biliyoruz. Burada önemli olan seçilen sayılar çok büyük olacağından bunların asal olup olmadığının kontrolünün nasıl sağlanacağıdır. Bunun içinde en çok kullanılanları fermat testi ve miller-rahin testi olan asallık testleri vardır.

Günümüzde RSA ile yaklaşık 300 basamaklı bir sayı başka bir deyişle 1024 bitlik bir anahtar ile şifreleme işlemi basit uygulamalar için yeterli olarak kullanılabilir.

Fermat Çarpanlara Ayırma Yöntemi ve bu yöntemden doğan diğer metotlar karşısında RSA' nın güvenilirliğini artırmak için RSA Sistemi'nde aynı bit genişliğinde olan asalların seçebilmesi uygun olacaktır.

p ve *q* asalları aynı bit üzerinde bulunurlar. Kaba koda karşı güçlü kalması için asal sayıların ikisinin de büyük olması gereklidir. Asalların aynı bit üzerinde alınmaya çalışılması, en iyi durumdur. Bunun nedenini ise şu şekilde açıklayabiliriz. Temeli çarpanlara ayırma zorluğuna dayanan RSA Şifreleme Metodu'nda çarpanlara ayırma ihtimali ne kadar zor olursa şifreyi kırmada o kadar zor olacağından bu algoritmada güçlü asal sayıları tercih etmek faydalı olacaktır. Bunun içinde *p* ve *q* asal sayılarını birbirine yakın uzunlukta seçmek çarpanlara ayırma ihtimalini zorlaştıracağı için algoritmanın güvenilirliğini arttıracaktır. Bu noktada seçilen bu *p* ve *q* asal sayıları 512 bitlik bir nodülde 256 bitlik tercih edilmesi en uygunu olacaktır.
Asallar arasında bit farkı olmadığından en uç örnek bulunulan bit değerinin en büyük ve en küçük değerlerine yaklaşmak amaçtır [13].

Şifreyi çözme aşaması, çarpanlara ayırma zorluğuna dayandığından dolayı şifreleme süresinden daha uzundur. Şifreleme ve deşifreleme hızlarını artırmaya yönelik bir takım yöntemler geliştirilmiştir. Şifrelemenin ana elemanı olan anahtar oluşturabilmek için yüksek güvenlik sağlamak adına seçilen çok büyük asal sayıları kullanalarak işlemin yapıldığı RSA Şifreleme Algoritması için 1985 yılında Montgomery tarafından kendi adını alan Montgomery algoritması tasarlanmıştır. Montgomery algoritmasının sadece yazılım noktasında iyi sonuçlar göstermemesinin sebebi, şifreleme aşamasında içerdiği işlem sayısı fazlalığıdır. Yapılan araştırmalar sonucunda da görüldüğü üzere bu algoritma, gerekli donanım desteği yapıldığında başarılı bir performans göstermiştir. Bu algoritma için işlem fazlalığı gibi dezavantajlı durumlardan biriside şifrelemede kullanılan anahtarın boyutunun büyük olmasıdır. Bu, algoritmanın hızını düşüren bir durumdur. Bu problemleri ortadan kaldırabilmek adına 1990 yılında Wiener tarafından Rebalanced CRT-RSA ve 2003 yılında da Paixo ve Alison tarafından R. Prime RSA Metodu Montgomery Algoritmasının geliştirilip daha iyi bir şekle getirilmesi sonucunda oluşturulmuştur. Ayrıca 1982 yılında Quisquater ve Couvreur tarafından sunulan CRT-RSA algoritması, RSA Algoritması'nın deşifreleme hızını yaklaşık 4 kat oranında arttırmıştır. Daha sonra 1997 yılında Collins vd. , şifreleme tekniği olarak CRT-RSA algoritmasını kullanarak metnin deşifrelenme kısmı için Multi Prime-RSA yöntemini sunmuşlardır. Yapılan performans ölçümleriyle en hızlı şifrelemenin standart RSA Algoritması'na göre 2,5 kat daha hızlı olan hızlı mod Alma algoritması kullanıldığında gerçekleştiği görülmüştür. Ayrıca anahtar oluşturmak için seçilen sayıların

büyüklüğünün artmasının, aradaki hız farkını da etkileyip artırdığı görülmüştür. Bir başka algoritma olan Binary Modüler Üs alma Algoritması ise Standart RSA Algoritması ile karşılaştırıldığında ortalama olarak 2 kat daha hızlı olduğu görülmüştür. Buradan da varacağımız sonuç şudur ki Standart RSA Algoritması ile karşılaştırılması yapılan Montgomery algoritmasının dışındaki diğer algoritmaların performans açısından bakıldığında Standart RSA'ya göre daha iyi olduğudur [28].

3.7. RSA Yöntemi ile Sayısal İmza

3.7.1. İmza şeması

Gelişen teknolojiyle birlikte internet ortamı üzerinde gereksinim duyulan sayısal imzalarda RSA şifreleme yöntemi uygulanır. (*e,n*) açık anahtarı ile yapılacak olan şifreleme işleminde metin $0 < m < n$ aralığında bir tamsayıya dönüştürülerek alıcısına ulaştıktan sonra *d* özel anahtarı ile deşifrelemeye tabi tutuluyordu [8].

3.7.2. RSA Metodunu Kullanarak İmzalama

Ali, Ayşe' ye bir ağ üzerinden ileti ulaştırmak isterse burada yapacağı işlem sadece kendisine ait olan gizli anahtarını kullanmak olacaktır. Uyguladığı *d* özel anahtarı ile imzalanmış olan veri, Ayşe'ye ulaştırılır. Böylece veri üzerinde elektronik imza işlemi gerçekleştirilmiş olur. Sonraki adım ise imzalanan veri üzerindeki imzanın onaylanması aşamasıdır [8].

3.7.3. İmza Onaylanması

Veri imzalandı ve Ayşe'ye ulaştı. Ayşe, sahip olduğu açık anahtarı kullanarak yaptığı matematiksel işlem sonucunda *m* değerine ulaşabilirse veri üzerine uygulanan imzanın doğruluğu tespit edilir [8].

4. BÖLÜM

RSA İLE İLGİLİ BİLGİLER

4. 1. RSA 'nın Kriptoanalizi

RSA Şifreleme Algoritması'nda anahtar oluşturmanın ilk adımı, çok büyük iki asal sayı seçerek ve bu iki asal sayının çarpılmasıyla oluşan ve yarı asal sayı olarak ifade edilen sayıyı kullanmaktır. Bahsi geçen bu yarı asal sayı şifreleme işlemindeki genel anahtarın bir parçasını oluşturur. Daha sonra $\varphi(n) < n$ ve $ebob(\varphi(n), n) = 1$ olan pozitif tam sayıların sayısı olarak ifade edilen $\varphi(n)$ değeri hesaplanır. Hesaplanan bu $\varphi(n)$ değeri ile aralarında asal olan ve bu $\varphi(n)$ değerinden küçük pozitif tamsayı olan bir *e* sayısı seçilir. Gizli anahtar olan '*d*' açık anahtarın bir parçası olan *e*'nin mod($\varphi(n)$)' e göre aritmetik tersidir. Böylece şifrelemede ve deşifrelemede kullanılacak olan anahtarlar oluşturulmuş olur. RSA Şifreleme Algoritması'nda şifreli metni deşifreleyebilmek için özel anahtar olan *d'* ye ihtiyaç vardır. Eğer ilk başta bahsedilen yarı asal sayının çarpanları bulunabilirse özel anahtar *d*' de bulunabilir. $\varphi(n)$)' nin rahatlıkla hesaplanabilmesi için *n* yarı asal sayısının çarpanlarına ayrılıyor olabilmesi gerekir. Daha sonra $e.d \equiv 1 mod\big(\varphi(n)\big)'$den özel anahtar *d* bulunur ve $M \equiv D(C) = m \equiv C^d \ (mod\ n)$ denkliği ile de asıl metne başka bir deyişle orijinal metne ulaşılabilir.

Çarpanlara ayırma algoritmaları iki gruba ayrılır. Bunlar genel amaçlı çarpanlara ayırma algoritmaları ve özel amaçlı çarpanlara ayırma algoritmalardır. Günümüz de hala RSA'nın kriptanalizi için kullanılan, çalışma zamanı verilen yarı asal sayısının büyüklüğü ile orantılı olan genel amaçlı çarpanlara ayırma algoritmaları şunlardır:

- "Quadratic sieve" - C. Pormanance, 1981.
- "General Number Field Sieve" - A.K. Lenstra, 1983.

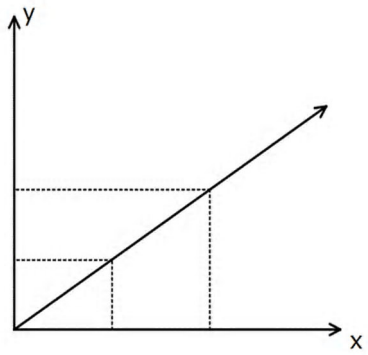
Çalışma zamanı verilen *n* sayısını oluşturan çarpanların veya *n* sayısının bazı belirli özelliklerine bağlı olmasından dolayı RSA Şifreleme Metodu'nda asal sayılar seçilirken ve *n* sayısı oluşturulurken göz önünde tutulması bir zorunluluk olan özel amaçlı çarpanlara ayırma algoritmaları bu yönüyle RSA da kullanılan yarı asal sayıyı oluştururken büyük öneme taşımaktadırlar. Günümüzde bilinen bazı özel amaçlı algoritmalar şunlardır:

• Trial division (Basit Bölme Algoritması)
• Fermat
• Euler ,
• Pollard
• Williams
• Eliptic curve [6]

4.2. RSA'nın Güvenilirliği

RSA Algoritması'nda anahtar boyu (key size) olarak adlandırılan şifreleme işlemi için tercih edilen iki asal sayı olan *p* ve q sayılarının çarpılmasıyla oluşan *n* sayısının boyutu büyüdükçe bu anahtarla anahtar ile şifrelenmiş metnin deşifreleme anahtarına sahip olmayan kişiler tarafından çözülmesi de güçleşir. RSA Security Şirketi ilk 1991 yılında RSA Çarpanlara Ayırma Problemini başlatmışlardır. Bu konuda en başarılı sonuca RSA-155 ile yani 155 haneli anahtar ile ulaşılmıştır. Bundan yedi ay sonra bir grup araştırmacı, 300 iş istasyonu ve PC'ler kullanarak bu görevi tamamlamıştır. 1995 yılında 512-bitlik şifrenin 1 milyon $' lık bir yatırımla sekiz ayda deşifrelenebileceğini iddia etmişlerdir. Fakat RSA-155 ancak 1999 yılında yedi ayda kırılabildi. O yıllarda internet üzerinden yapılan e-ticaret uygulamalarında 512-bitlik şifreleme uygulanıyor olmasından dolayı bu şifrenin kırılması önemliydi. 2010 yılı içerisinde RSA Security Şirketi 768 bitlik şifrenin 6 ayda 100.000 iş istasyonu ile deşifrelendiğini bildirmişlerdir. Verinin değerine ve değerini koruma süresine göre 768 bitlik şifrelerin halen daha uygulanabileceğini söylemişlerdir. Bununla birlikte, 1024 bitlik bir şifrenin 10 yıl sonra deşifrelenebileceğini düşünmenin bile çok iyimser olacağını ifade eden bu şirket 1024-bit RSA Şifreleme'nin çözülmesinin 768-bit modülüne göre çok daha zor olduğunu duyurdu. *n* sayısının çarpanlarına ayrılabilmesi tehdidinin yanında "seçilmiş metin saldırısı" da tüm asimetrik sistemlere karşı kullanıldığı o gibi RSA kriptografisine karşıda kullanılabilir. Asimetrik şifreleme sistemlerinde saldırgan herhangi bir şifreleme

işlemini gerçekleştiren kişinin açık anahtarını görebilir. Saldırgan buradan yola çıkarak, açık anahtar ile kendi oluşturduğu bir mesajı şifreler. Daha sonra şifrelediği bu metin üzerinde anahtar uzayının olabilecek bütün özel anahtarlarını deneyerek şifreyi çözmeye, kendi belirlediği orijinal metne yeniden ulaşmaya çalışır. Buradaki amaç, sadece alıcıda var olan özel anahtarı bularak asıl şifreyi kırmaktır [3, 30]. Buradan da anlaşıldığı üzere RSA'nın güvenliği yine *n* sayısı ile doğru orantılıdır. Yani anahtar uzayının büyüklüğünü *n* sayısının büyüklüğü belirlemektedir.



Şekil 3. 5. Anahtar uzayının büyüklüğü ile *n* sayısının büyüklüğü arasındaki ilişki
x: anahtar uzayının büyüklüğü
y: *n* sayısının büyüklüğü

Burada önemli olan, RSA bu güvenilirliği sağlarken iletişim sistemlerinin bazı özellikleri sağlaması gerekir. Yani metnin güvenli bir şekilde, değiştirilmeden alıcısına ulaşması, alıcısının da şifreli metni değişime uğramadan alabilmesi için kriptolojik sistemin aşağıda bahsi geçen unsurları sağlaması gerekir.

4.2.1. Gizlilik

İletişim sistemini ulaşılması istenen kişiler dışındaki kimselerden gizli tutarak sistem güvenliğini korumayı amaçlar. Metin şifrelenip iletildiği ana kadar geçen sürede oluşabilecek üçüncü kişi saldırılarına karşı sistemin gizli kalmasıdır [1].

4.2.2. Bütünlük

Tez boyunca şifreleme algoritmasının birçok saldırıya maruz kalacağından bahsettik. Saldırı yapan kişi bir takım saldırı metotlarıyla şifreyi kırıp düz metne ulaşabilir.

Ulaştığı metni değiştirip alıcıya bambaşka bir metin gönderebilir. İşte bütünlük ilkesi iletilecek metnin değiştirilmeden, bir kısmının silinmeden ya da bilgi eklemesi yapılmadan ilk hali olarak bütün bir şekilde ulaştırmayı amaçlar [1].

4.2.3. Kimlik Denetimi

Gönderici, iletiyi güvenli ve bütünlük ilkesi çerçevesinde göndermiş yerine ulaştırmış olsun. Ancak doğabilecek sıkıntılar burada bitmemektedir. Alıcı, mesajı gerçekten olması gereken kişinin gönderip göndermediğinden emin olmak ister. Bu noktada, kimlik denetimi unsuru ortaya çıkar. Sağlanan kimlik doğrulamasıyla alıcı gönül rahatlığı ile metni deşifreler [1].

4.2.4. İnkâr Edememe

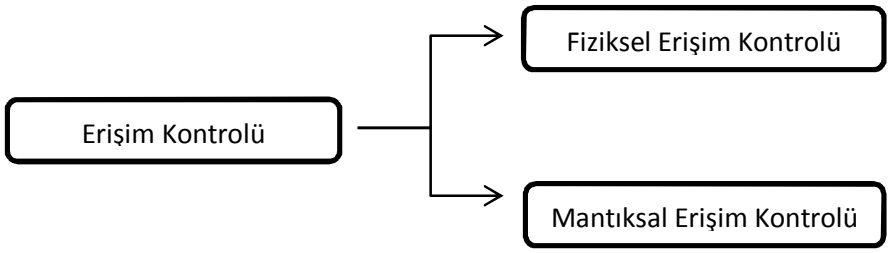
Bu özellikle gönderici mesajı göndermedim, alıcıda almadım diyemez. Bu metnin gönderilip alındığının ispatıdır. Bu noktada dijital sertifikalar ve dijital imzalar devreye girer. Gerekli ispat dijital imza ile sağlanır. Metin üzerinde bir değişiklik söz konusu oldu ise hem gönderici hem de alıcı bu değişikliği kabul eder [1].

4.2.5. İletişim Sisteminde ki Erişim Kontrolü

Şifreli iletişim sisteminde kimlerin hangi veriye ulaşabileceğini, kimlerin hangi verileri kullanabileceğini belirleyen bir güvenlik tekniği olan erişim kontrolü uygulandığı alana göre iki alt başlıkta incelenir. Bunlar:

1. Fiziksel Erişim Kontrolü
2. Mantıksal Erişim Kontrolü

dür [1].



Şekil 4. 1. Erişim kontrolünün alt dalları

Peki, bu güvenlik teknikleri hangi alanlarda erişim denetimi uygular bir göz atalım. Fiziksel erişim denetimi kampüs oda bina ve fiziksel IT varlıklarına ulaşım kısmını denetler ve sınır koyar. Mantıksal erişim denetimi ise bilgisayar sistemlerine, sistemdeki dosyalara ve bilgilere olan bağlantıyı kontrol altında tutar [1].

4.3. RSA'ya Karşı Yapılan Saldırılar

1970' lerden beri kullanılmakta olan RSA Şifreleme Metodu, kullanılmaya başlanıldığı günden bu güne kadar geçen surede yaygınlaşmış ve kullanım alanı genişlemiştir. Diğer şifreleme metotlarına oranla kullanım açısından daha çok tercih edilmekte ve bundan dolayı da amacı gizli anahtar ile ilgili bilgi edinerek orijinal metne ulaşmak olan birçok deşifreleme saldırılarına maruz kalmaktadır. Peki nedir bu saldırı?

Şahsi zevk, popülerlik kazanma, ulaştığı bilgilerden maddi kaynak sağlama, bir başkası için ajanlık yapma ve terör sebebiyle yapılan amacı iletişim esnasında oluşan iletim akışını engellemek veya sistemi komple çökertmek olan saldırı kasıtlı olarak şifreli bilginin üçüncü kişiler tarafından ele geçirilip imha edilmesi ya da kullanılması iletişim sistemine zarar verilmesidir. Saldırıyı gerçekleştiren kişiye ise saldırgan adı verilir. Herhangi bir ülkeden ve herhangi bir sunucudan doğabilecek olan saldırılar, dış saldırgan olarak adlandırılırken veri kaynağına dış saldırgana göre daha yakın olan ve bu açıdan dış saldırgana göre daha da zararlı olabilecek saldırılar, iç saldırgan olmak üzere iki tip saldırgandan bahsedebiliriz. External saldırganlar olarakta bilinen dış saldırganların hakkında pek fazla bilgi yoktur ve bu kişiler saldırılarını bir ağ üzerinden genellikle bir araçtan faydalanarak gerçekleştirirler. Öte yandan internal saldırgan olarakta ifade edilen iç saldırganlarda veriyi direk kullanabilme olasılıkları söz konusu olduğu için daha fazla tehlike arz ederler [1]. Kimdir bu saldırganlar ondan bahsedelim.

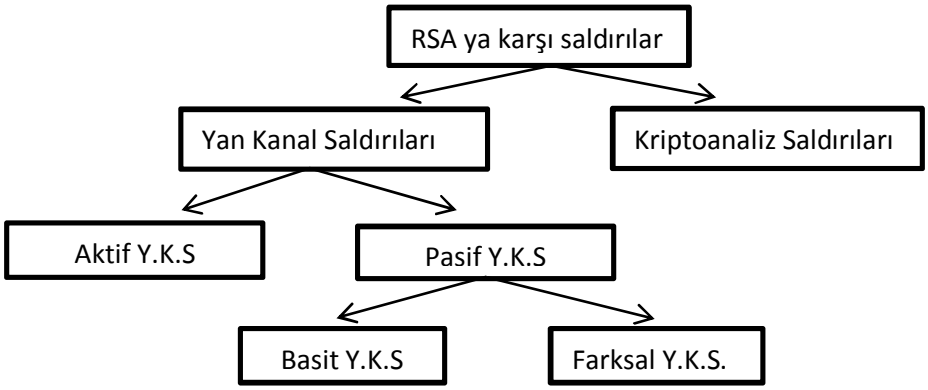
- Network kullanıcıları
- Ajanlar
- Suçlular
- Teröristler
- Kaynaksız bir başka deyişle bilinmeyen saldırganlar
- Hackerler

Ayrıca saldırganları iç ve dış saldırganların dışında amatör ve profesyonel saldırgan olarak sınıflandırmamız mümkündür. Genel hatlarıyla bir sisteme yapılan saldırıları dört başlıkta sınıflandırabiliriz. Bunlar:

- Aktif ataklar
- Pasif ataklar
- Password atakları
- Kod ve Kriptografik ataklar [1].

Bu saldırıları RSA şifreleme algoritması açısından ele alalım. RSA Sistemi'ne en çok zarar verecek saldırı, bir kriptoanalistin belli bir açık anahtara karşı gelen gizli anahtarı bulmasıdır. Bunu başarabilen bir düşman, hem şifrelenen bütün masajları deşifreleyebilir, hem de imzaları taklit edebilir. Bunu yapmanın en akla gelen yolu *n*'nin asal çarpanlara ayrılması yani *p ve q*'nun hesaplanmasıdır. *p, q* ve açık üs *e* kullanılarak özel anahtar *d* kolaylıkla hesaplanabilir. RSA algoritmasına karşı yapılan bazı saldırılar vardır. RSA Şifreleme Yöntemi'ne karşı yapılan bu saldırılar için Dubey,Raten,Verma-Saxena olmak üzere bit takım metotlar geliştirilmiştir Bu saldırıları iki başlık altında sınıflandırmak mümkündür.

1. Yan kanal saldırıları
2. Kriptoanaliz saldırıları



Şekil 4. 2. RSA kriptografik sisteme karşı yapılan saldırılar

Aktif ve pasif olmak üzere iki şekilde incelenen yan kanal saldırıları, algoritmaların çalıştığı ortamın sağladığı bilgiler kullanılarak deşifrelemeye çalışılan saldırı yöntemidir [13].

Pasif yan kanal saldırılarında sisteme herhangi bir müdahale yapılmaksızın algoritmanın çalışması sırasında istemsiz olarak dışarıya sızan bilgilere ulaşılması bununla da orijinal metnin çözülmesi amaçlanmıştır [13].

Pasif yan kanal saldırılarına göre daha zor ve pahalı bir uygulama gerektiren aktif yan kanal saldırılarında ise algoritmanın çalıştığı sisteme dışardan bir müdahale vardır. Ayrıca bu saldırı türünde diğer türden farklı olarak saldırı yapıldığına dair bir ipucu kalmaktadır [13].

Pratikte her iki saldırı yöntemini kullanarak RSA' nın kırılması çok zordur. Çünkü oluşabilecek her türlü saldırıya karşı çok daha büyük asal sayılar kullanılarak şifreleme yapılmaktadır. Öyle ki bu asal sayılara ulaşmak ağır matematiksel işlemleri gerektirmektedir.

Biz bu noktada basit ve farksal olmak üzere iki çeşidi olan bütün pasif yan kanal saldırılarından bazılarına değineceğiz. Bu saldırılar kullanılan yan kanal bilgisine göre 4 başlık altında incelenir. Saldırı türlerinde kaynak [16, 24] dan yararlanılmıştır.

4.3.1. Zamanlama Saldırıları

Amerikalı kriptocu olan Paul Carl Kocher tarafından 1995 yılında bu alanda yapılan ilk çalışma olan zamanlama saldırıları, şifreleme işleminin işlem basamaklarının herhangi bir adımında yapılan işlemin süresine bakarak bu süreye göre tespitler yapmayı temel alan bir saldırı türüdür. Başka bir deyişle şifreleme işlemini yapan cihazın yaptığı işlem basamaklarıyla ilgili zaman farklılıklarından çıkarımlar yapılarak gizli anahtarın bulunarak orijinal metnin deşifre edilmesine yönelik yapılan saldırıdır. Bu saldırı türünde 2000 yılında Werner Schindler çinli kalan teoremi ile RSA Algoritması'na karşı bir saldırı gerçekleştirilebileceğini ifade etmişlerdir. Bunda üç yıl sonrada Brumley ve Boneh tarafından yapılan çalışma, ilerde bir ağ üzerinden elde dilen bilgiler ile RSA ya karşı başka bir saldırı yapılabileceğini göstermişlerdir. Tabi ki bu saldırıların önüne geçmek gerekli tedbirleri almakla mümkün olacaktır. Yapılması gereken şifreleme metodunda yapılacak olan her bir işlemin normal işletim sürecinde gerçekleşebilecek şekilde tasarlanmasıdır.

4.3.2. Güç Analiz Saldırıları

Elektromanyetik alanda meydana gelen akım farkından yararlanılarak veri elde etmeye çalışılarak bu verilerle düz metne ulaşmak amaçlanmıştır.

4.3.3. Akuistik (ses) Saldırıları

2004 yılında Shamir tarafından geliştirilen akuistik kriptoanaliz metodunda, RSA Şifreleme Algoritması'nın şifreleme ve deşifreleme aşamalarında artan matematiksel işlemlerden dolayı cihazdan çıkan bazı seslerin geliştirilen aletler ile dinlenip çıkarımlar yapılarak ana metne ulaşma amaçlanır.

4.3.4. Elektromanyetik Analiz Saldırıları

Kriptografik cihazın algoritma çalıştığı esnada meydana gelen elektromanyetik yayılımın incelenip veri elde edilmesiyle yapılır. Daha başka saldırı türlerine de göz atacak olursak

4.3.5. Çarpanlara Ayırma Saldırısı

Kaba kuvvet saldırısı olarak bilinen klasik şifre çözme yöntemini RSA' ya uyarlanmış versiyonu olan çapanlara ayırma saldırı kısmında İlk olarak deneme yöntemi ile çarpanlara ayırma metoduna göz atacak olursak:

Direk yöntemlerden biri olan deneme yöntemi ile çarpanlara ayırma, herhangi bir n sayısını kısmen veya tamamen çarpanlara ayırmada kullanılan hem etkili hem de basit bir yöntemdir. Çarpanlara ayırmak istediğimiz sayıyı en küçük asal sayıdan başlayarak kendisine kadar mevcut olan bütün asal sayılara bölünüp bölünemeyeceğinin tek tek hesaplanması yöntemidir. Bu yöntemin tercih edildiği durum çarpanlara ayırmak istediğimiz sayının büyük seçilmediği durumdur.

Diğer bir çarpanlara ayırma yöntemi olan fermat yöntemini, RSA Şifreleme Algoritması'na saldırı tehdidi açısından değerlendirelim. Bu yöntem güvenirliliği çarpanlara ayırma zorluğuna dayanan RSA Algoritması gibi algoritmalara saldırı için kullanışlı bir yöntemdir. Fermat çarpanlara ayırma, iki kare farkı oluşturmaya dayanır. Başka bir deyişle her hangi bir n sayısını ele alalım. Seçilen bu sayı iki kare farkı olarak yazılabilirse bu n sayısının çarpanları $(a+b).(a-b)$olarak elde edilmiş olur. Çarpanlara ayırmak için bu çiftin yeterli olduğu fermat yönteminde eğer çarpanlar birbirine yakınsa

bu yöntem çok iyi çalışır. Eğer çarpanlar birbirine yakın değilse yani tersi durum söz konusu ise bu yöntemin zayıf kaldığını söyleyebiliriz. Bu metotlardan başka kullanılan diğer çarpanlara ayırma metotları ise aşağıda ifade edildiği gibidir.
Eliptik eğri yöntemi (eliptik eğriler şifreleme algoritmalarında oldukça çok ve güncel kullanım alanına sahiptir)

4.3.6 İkinci Dereceden Kalbur Yöntemi

Bu yöntem özellikle verinin güvenliği ve saklanması aşamasında zorluğu çarpanlara ayırma esasına dayanan şifreleme yöntemlerine karşı saldırı için kullanılır.
. Atkin Kalburu
İsmini 2004 yılında bu yöntemi inceleyen ve geliştiren kişiden ala daha önceden bu problemle ilgilenen eratosten tarafından incelenen çözümün ilerlemiş versiyonu olan bu yöntem belirli bir aralıkta seçilen bütün asal sayıları bulmaya yarayan bir algoritmadır.
. Pollard Rho Yöntemi
Bu yöntem verinin güvenliği açısından oldukça önemlidir. Bu yöntemin amacı, büyük asal sayıların hızlı olarak çarpanlara ayırmaktır.
. Ters Kalbur Çarpanlara Ayırma

4.3.7. Küçük e Saldırısı

Bilindiği üzere RSA Şifreleme Yöntemi'nde şifreleme işlemi için bir *e* sayısı kullanılıyor. Bu *e* sayısını çok küçük bir sayı tercih edildiğinde şifrenin kırılma olasılığı da artacaktır. Küçük seçilen bu *e* sayısı ile birçok kişiye metin şifreleyip gönderildiğinde şifreyi kırmak için uğraşan kişi işlem akışını dinlerken elde ettiği bilgiler ile çinli kalan teoremini kullanarak şifreyi çözüp orijinal metne ulaşabilir.

4.3.8. Kuantum Hesaplama Gücü İle Yapılan Saldırılar

1994 yılında Peter Sher, kuantum bilgisayarlar üzerinde çalışan ve *n* sayısının çarpanlara ayrılmasını sağlayan Sher algoritmasını ifade etmiştir. Kendine verilen sayının çarpanlarını çıktı şeklinde üretmek esasına dayanan Sher algoritmasının duyurulmasıyla birlikte başka bir deyişle kuantum bilgisayarlarının gelişmesiyle birlikte RSA Algoritması'nın deşifre edilmesi mümkün olacaktır.

4.3.9. Hata Analizi Saldırıları

2010 yılında RSA Algoritması'nı kırmaya yönelik yapılan bir saldırı çeşidi olan hata analiz saldırısında ise algoritma uygulanırken bazı parametreler sıcaklık, ışık gibi çevreden kaynaklı etkenlerle değiştirilmesi sağlanarak hatalı çalışmaya zorlanan sistemden elde edilen verilerin karşılaştırılarak şifreyi kırmayı amaçlar.

SONUÇ VE ÖNERİLER

Sonuç olarak bilginin başkaları tarafından ele geçmeyecek şekilde güvenliğinin sağlanması için geliştirilen yöntemler, her geçen gün önem kazanmaktadır. Bilgi korunumu amacıyla yapılan şifreleme işlemleri, günümüzde hayatımızın her anında karşımıza çıkmaya başlamış bu sebeple de gerek simetrik şifreleme yöntemi gerekse asimetrik şifreleme yöntemi ile bunlar içinde özelliklede RSA Şifreleme Metod'u sık sık kullanılma gereksinimini doğurmuştur. Güvenli iletişimde kırılma ihtimali düşük olan RSA ya olan tercih her geçen gün artmıştır. Bu yüzden de RSA'nın hızını artırmaya yönelik çok daha kapsamlı çalışmalar yapılabilir ve bu uygulama daha kullanılabilir bir hale getirilebilir.

KAYNAKLAR

1. Aghayev M., "Kriptoloji ve Veri Şifreleme Teknikleri Üzerine", Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir (2017).

2. Altındiş H., "Sayılar Teorisi ve Uygulamaları', (2. Basım), Ankara.

3. Aksuoğlu A., "RSA Algoritmasının İyileştirilmesi İçin Yeni Bir Yaklaşım", Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı (Eylül-2010).

4. Arda, D., "Kodlama teorisinin kriptografik açıdan incelenmesi", Doktara Tezi,Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, 30-32 (2011).

5. Bilişim Teknolojileri Dergisi, Cilt: 6, Sayı: 2, (Mayıs 2013).

6. Bütün N., "RSA Kripto Sistemi ve *p-1* Çarpanlara Ayırma Algoritması" Yüksek Lisans Tezi, Erzincan Binali Yıldırım Üniversitesi Fen Bilimleri Enstitüsü, Erzincan (2018).

7. Çıkıkçı Ş., "Asimetrik Şifreli Sistemlerin Uygulamaları ", Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne (2010).

8. Çetinkaya H., "RSA ve Elgamal Kısmi Homomorfik Kripto Sistemlerin Vergi Ödeme Sistemine Uygulanması ve Bu Uygulamaların Performans Analizleri", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Bilişim Enstitüsü (Haziran 2019).

9. Çimen C., Akleylek S. ve Akyıldız E. (2002).

10. Demir İ., "RSA Algoritmasının Üç çekirdekli Leon3 İşlemcisi Tabanlı Sistem Üzerinde Hata Enjekte Etme Atağına Dayanıklı Gerçeklenmesi", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü (Mart 2018).

11. Erzurumlu Z., " Simetrik ve Asimetrik Kripto Sistemler ", Yüksek Lisans Tezi,Matematik Anabilim Dalı, Erzurum (2013).

12. Hassanpour A.A., "Asal Sayıların Şifreleme Teorisindeki Uygulamaları ",Yüksek Lisans Tezi, Atatürk Üniversitesi Fen Bilimleri Enstitüsü, Erzurum (2015).

13. Hatun E., "Raspberry Pı Üzerinde Gerçeklenmiş RSA Algoritmasına Yan KanalAnalizi", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü (Nisan 2018).

14. İnternet:Wikipedia, "Kriptoloji", **http://tr.wikipedia.org/wiki/Kriptoloji** (2013).

15. Okumuş İ., "RSA Kriptosistemi'nin Hızını Etkileyen Faktörler", Doktora Tezi, Atatürk Üniversitesi Fen Bilimleri Enstitüsü, Erzurum (2012).

16. Kaya U., "PC Çözümleri: RSA Algoritması", **Tübitak SGE** (Mart 2014).

17. Kodaz H., Botsalı F.M. , "Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması" , **Selçuk Teknik Dergisi, Cilt9,** Sayı:1 (2010).

18. Akleylek S., Yıldırım H.M., Yüce Tok Z., **'Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri'**, İnönü Üniversitesi (2 – 4 Şubat 2011).

19. Lüy E., "Homomorfik Kriptosistemler ve Özellikleri Üzerine", Doktora Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Kayseri (2015).

20. Nasıbov S., "Kriptoloji Sistemleri ve Uygulamaları Üzerine", Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir (2015).

21. Obaıd Z., "Kriptoloji Yöntemlerinin Karşılaştırılması", Yüksek Lisans Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Kayseri (Nisan 2016).

22. Özdemir D., Beşkirli A. , Beşkirli M. , "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme", **Avrupa Bilim ve Teknoloji Dergisi Özel Sayı**, S. 284-291 (Ekim 2019).

23. Özyılmaz Ç., "Kriptolojiye Giriş ", Yüksek Lisans Tezi, Karabük Üniversitesi Fen Bilimleri Enstitüsü, Karabük (2014).

24. Şaykol E., Altıner H. , "Veri Güvenliğinde Tempest Saldırı Türleri Üzerine Tarihsel Bir İnceleme" , **Beykent Üniversitesi Fen ve Mühendislik Bilimleri Dergisi Cilt 6**(2), 121-152, (2013).

25. Ulutürk A., "Gelişmiş Şifreleme Standardı" , Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara (2010).

26. Ülker Ü., "Klasik Teknikler Kullanılarak Bir Kriptografi Algoritması Geliştirilmesi ve DES Algoritması ile Performans Analizlerinin Karşılaştırılması" , Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara (2014).

27. Yerlikaya, T., Buluş, E., Buluş, N., **"Kripto Algoritmalarının Gelişimi Ve Önemi Akademik Bilişim Konferansı'**, Denizli (2006).

28. Yerlikaya T., Aslanyürek C., "RSA algoritmasının şifreleme hızını arttıran algoritmalar ve performansları", **DÜMF Mühendislik Dergisi 10:3**, (2019)

29. Yeşilbaş E., "Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları", Yüksek Lisans Tezi, Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü, Rize (2016).

30. Yıldırım K., "Veri Şifrelemesinde Simetrik ve Asimetrik Anahtarlama Algoritmalarının Uygulanması", Yüksek Lisans Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Kocaeli (2006).

31. Yılmaz R., "Kriptolojik Uygulamalarda Bazı İstatistik Testler" .Yüksek Lisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya (2010).

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı, Soyadı : Sümeyye ENGİN
Uyruğu: Türkiye : (TC)
Doğum Tarihi ve Yeri: 24 Ekim 1989, Kayseri
Medeni Durumu : Evli
Email : alvina@erciyes.edu.tr
Yazışma Adresi : Kayseri Merkez PTT/KAYSERİ

EĞİTİM

Derece	Kurum	Mezuniyet Tarihi
Yüksek Lisans	EÜ Fen Bilimler Enstitüsü	2020
Lisans	EÜ Fen Fakültesi, Matematik	20012
Lise	Sümer Lisesi, Kayseri	2007

İŞ DENEYİMLERİ

Yıl	Kurum	Görev
20013- Halen	PTT	Memur