Rest/Rest API

- 2017 BİLGİ GÜVENLİĞİ FINAL -

① - $p=5$, $q=11$, $e=3$, $x=9$ için RSA ile

a-) metni şifreleyin (25)

b-) şifrelenmiş metni çözün (25)

② - Bir saldırgan saniyede 5×10^8 tuş deneyebiliyor. Bunun için özel bir ASIC üretiliyor. Bir ASIC'in maliyeti 50$'dır. 1 milyon dolarlık bütçe ile kaç tane paralel ASIC çalıştırabiliriz. Evrenin yaşıyla ilişkilendirin (10^{10} yıl) (25)

b-) Bilgisayar Devresinin her 18 aydа bir 2 kat arttığını varsayarsak 24 saat'le indirmek için 128 bitlik AES'i kırmak ne kadar sürer (25)

No:

Adı Soyadı:

Bilgi Güvenliği Dersi Bütünleme Sınavı

1- Verilen RSA algoritmasının parametreleri p=5, q=11, ve e=3 şifrelenecek metin ise **9**

   a- Verilen planitexti şifreleyiniz? **(20 puan)**

   b- a şıkkında elde ettiğiniz ciphertext'in şifresini çözünüz? **(20 puan)**

2- Z_6'e göre 3'ün ve 5'in çarpmaya göre tersleri nelerdir? **(20 puan)**

3- Her biri 50 TL olan ve saniyede 5.10^8 tane AES şifresi deneyebilen entegreler bulunmaktadır. Saldırgano
1.000.000 TL para vardır 128 bitlik AES algoritması kullanılmaktadır.

   a- En fazla ne kadar sürede bu algoritma kırılabilir.(Hesapları nasıl yaptığınız önemli. Sonuçları üslü biç
   verebilirsiniz) **(20 puan)**

   b- Moore kanunu: her 18 ayda bir işlemcilerin hızı 2 kat artmaktadır. Bu kanunan göre a şıkkında verile
   sorunun 24 saatte çözülebilmesi için kaç yıl geçmesi gerekir. .(Hesapları nasıl yaptığınız önemli. Son
   üslü biçimde verebilirsiniz) **(20 puan)**

Ba
07.0
Doç. Dr. Ahmet Bedr

İsim:

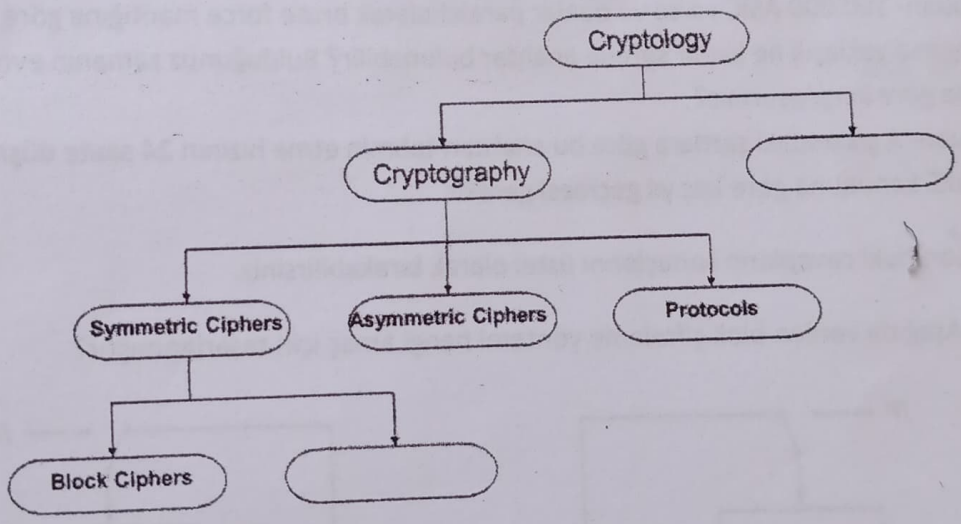
Numara:

1	2	3	4	5	Toplam

Bilgi Güvenliği Dersi TEK DERS Sınavı

1- Bir Simetrik Şifreleme sisteminin Brute Force saldırılarına dirençli olması için anahtar uzunluğu en az kaç bit seçilmelidir?

2- Aşağıda verilen şekilde Boş olan 2 kutucuğu soru üzerinde doldurunuz?



3- Hash fonksiyonlarında preimage resistance nedir. Açıklayınız?

4- RSA şifreleme algoritmasında **anahtar üretimini** anlatınız? Sayısal örnek ile de anlatabilirsiniz?

5- DES algoritmasında planitext ve anahtar tamamen 0 lardan oluşuyorsa, ilk tur (round) sonunda ne elde edilir?

Başarılar.

13-06-2017

CEVAPLAR

ADI SOYADI:

NO:

BİLGİ GÜVENLİĞİ ARASINAVI **20.03.2017**

1- **25 puan**- DES algoritmasında planitext ve anahtar tamamen 0 lardan oluşuyorsa, ilk tur (round) sonunda ne elde edilir?

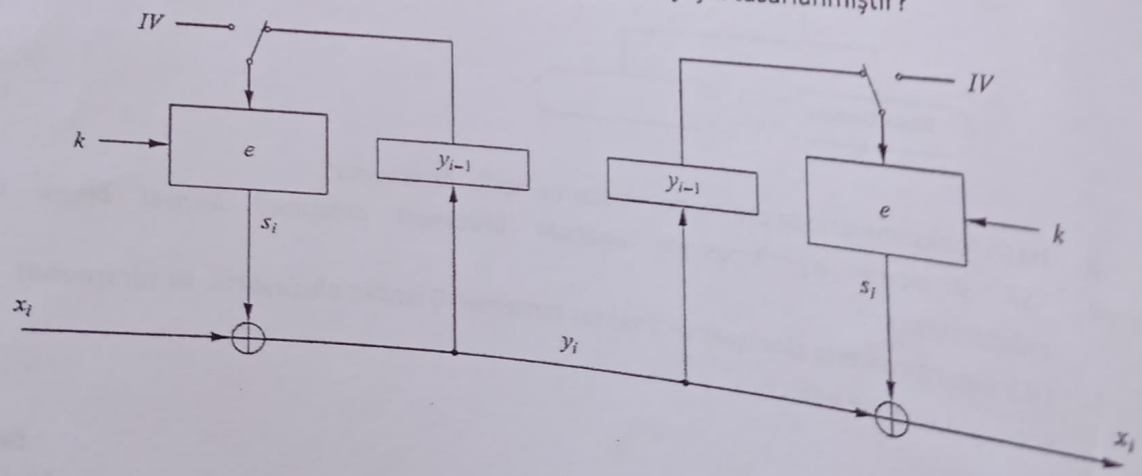
2- 192 bitlik anahtara sahip AES algoritmasını düşünelim. Saniyede 3.10^7 şifre deneyen ASIC (özel entegreler) olduğunu varsayalım. Evrenin tahmin edilen yaşının yaklaşık 10^{10} yıl olduğu kabul edilmektedir. Moore kanununa göre her 1.5 yılda bilgisayarların hızı 2 kat arttığı varsayılmaktadır. Tüm bu bilgiler ve varsayımlar ışığında;

   a- **25 puan**- 100.000 ASIC varsa ve bunlar paralel olarak brute force mantığına göre şifreleri deniyorsa yaklaşık ne kadar sürede anahtar bulunabilir? Bulduğunuz zamanın evrenin yaşına göre karşılaştırınız?

   b- **25 puan**- A şıkkındaki şartlara göre bu anahtarı tahmin etme hızının 24 saate düşmesi için MOORE kanununa göre kaç yıl geçmesi gerekir.

   NOT: Bu sorudaki cevapların sonuçlarını üstel olarak bırakabilirsiniz.

3- **25- puan** Aşağıda verilen blok şifreleme yöntemi hangi amaç için tasarlanmıştır?



Başarılar

No:

Adı Soyadı:

Bilgi Güvenliği Dersi Ara Sınavı

1- Verilen RSA algoritmasının parametreleri p=5, q=11, ve e=3 şifrelenecek metin ise 9
   a- Verilen planitexti şifreleyiniz
   b- A şıkkında elde ettiğiniz ciphertext'in şifresini çözünüz
2- Her biri 50 TL olan ve saniyede 5.10^8 tane AES şifresi deneyebilen entegreler bulunmaktadır. Saldırganda 1.000.000 TL para vardır 128 bitlik AES algoritması kullanılmaktadır.
   a- En fazla ne kadar sürede bu algoritma kırılabilir.(Hesapları nasıl yaptığınız önemli. Sonuçları üslü biçimde verebilirsiniz)
   b- Moore kanunu: her 18 ayda bir işlemcilerin hızı 2 kat artmaktadır. Bu kanunan göre a şıkkında verilen sorunun 24 saatte çözülebilmesi için kaç yıl geçmesi gerekir. .(Hesapları nasıl yaptığınız önemli. Sonuçları üslü biçimde verebilirsiniz)

Başarılar

27.04.2015

Doç. Dr. Ahmet Bedri ÖZER

SORULAR

1) $p = 5$, $q = 11$, $e = 3$, $x = 9$ için RSA ile

a) metni şifreleyin

b) şifrelenmiş metni çözün

çözüm

a) 1) $p = 5 \quad q = 11$

2) $n = p * q \longrightarrow 5 * 11 = 55$

3) $\Phi(n) = (p-1) * (q-1) = 4 * 10 = 40$

4) choose $= e = 3$

5) $d = e^{-1} = \bmod 40$

$3 \cdot 3^{-1} = 1 \bmod 40$

$27 \cdot 3 = 81 \mid 40$

$81 \mid 2$

0

$3^{-1} = 27$

$d = 27$ //

$y = x^e = 9^3 \longrightarrow 729 \bmod 55$ $\quad$ Kpub $= (n, e) = (55, 3)$

b)

$729 \mid 55$

$-715 \mid 13$

14

$y = 14$

$y^d = 14^{27}$

$14^{27} \equiv x \bmod 55$

$x = 9$ //

2) $\mathbb{Z}_6$'ya göre 3'ün ve 5'in carpmaya göre tersleri nelerdir?

Cevap

gcd(a,m) ≡ 1 ise $\mathbb{Z}_m$'deki bir sayının carpmaya göre tersi vardır.

Aralarında asal → iki ya da daha fazla sayının 1'den başka ortak böleni olmaması //

$\mathbb{Z}_6$'ya göre dediğine göre; 3'ün tersi yoktur çünkü 6 ile aralarında asal değildir.

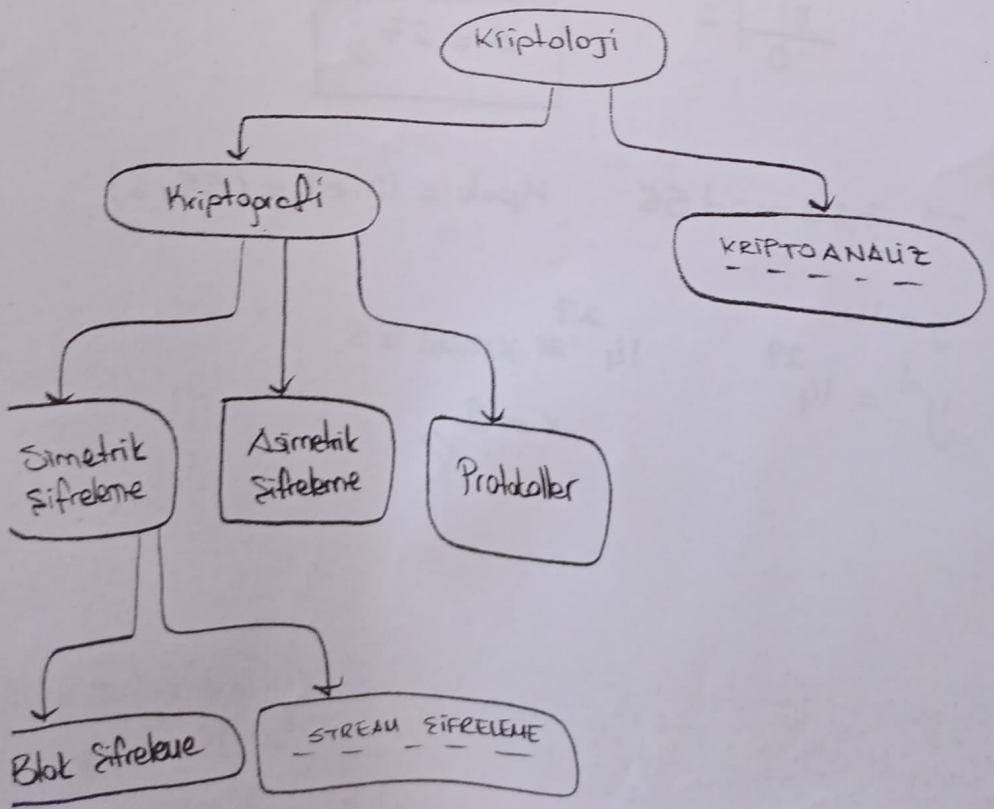
$5 \cdot 5^{-1} \equiv 1 \bmod 6$

$5 \cdot 5 \{25 \mid 6$

1

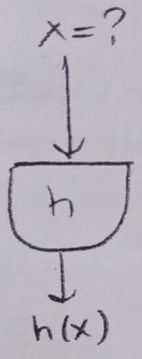
$5^{-1} = 5$ } 5'in tersi 5'tir

3) Aşağıda verilen şekilde boş olan 2 kutucuğu soru üzerinde doldurunuz.



4) Hash fonksiyonlarında preimage resistance nedir. Açıklayınız.

Cevap :



* Tek yönlü olmalı
* Geri yönlü olmamalı

$y = f(x)$
$x = f^{-1}(y)$ } sağlamamalı

* Tekrar eski mesajı elde etmeye çalışmamalı.

5) RSA şifreleme algoritmasında anahtar üretimini anlatınız? Sayısal örnek ile de anlatabilirsiniz.

Cevap :

public key: Kpub=(n,e) private key : Kpri = d

1. p ve q asal seçilecek (büyük sayı seçilecek)
2. $n = p * q$
3. $\phi(n) = (p-1) * (q-1)$
4. $\phi \in \{1, 2, \dots \phi(n-1)\}$
5. $d * e = 1$
6. return kpub = (n, e) kpri = d

6) Bir simetrik şifreleme sisteminin BruteForce saldırılarına dirençli olması için anahtar uzunluğu en az kaç bit seçilmeli?

Cevap : Eğer anahtar 64 bit seçilirse birkaç güne kaba kuvvet algoritması ile bulunur. Ama 128 bit veya 256 bit seçilirse bulunması yıllar alır. En düşük 2^{80} olmalı.

7) DES algoritmasında plaintext ve anahtar tamamen 0'lardan oluşuyorsa, ilk tur (round) sonunda ne elde edilir?

Cevap: DES'in çalışma mantığı metni parçalara (bloklara) bölüp harflere göre şifreleme yapıyor. Metin de anahtar da sıfırsa tur da sıfır çıkar.

8) Her biri 50 TL olan ve saniyede 5.10^8 tane AES şifresi deneyen entepreler bulunmaktadır. Saldırganda 1.000.000 TL para vardır 128 bitlik AES algoritması kullanılmaktadır.

a) En fazla ne kadar sürede bu algoritma kırılabilir. (Hesapları nasıl yaptığınız önemli. Sonuçları üslü biçimde verebilirsiniz)

Cevap: Entepreların her biri → 50 TL

1.000.000 TL var $= \frac{\text{Toplam para değeri}}{\text{Bir entepreninparası}} = \frac{1.000.000}{50} = 20.000$ tane entepre

→ 128 dediği $= 2^{128}$ komut

→ Entepreların çarpımı $= 20.000 \times 5.10^8 = 10^{13}$

$\frac{2^{128}}{10^{13}} = 3,402 \times 10^{29}$ sn → $\frac{3,402 \times 10^{25}}{365.24.60.60} = 1.079.10^{18}$ yıl geçmesi gerek

Evrenin yaşını istiyorsun!

b) Moore kanunu: her 18 ayda bir işlemcilerin hızı 2 kat artmaktadır. Bu kanuna göre a şıkkında verilen sorunun 24 saatte çözülebilmesi için kaç yıl gerekir?

Cevap: 24 saat ⇒ 24.60.60 = 86400 sn → $\frac{\text{komut}}{\frac{\text{kN}}{\text{sn}}} = \text{sn}$

$\frac{2^{128}}{x} = 86400$ sn $\quad x = 3,938.10^{33}$ $\frac{\text{komut}}{\text{sn}}$ = işlemci hızı

$\frac{\text{Gerekli işlemci hızı}}{\text{mevcut işlemci hızı}} = \frac{3,938.10^{33}}{10^{13}} = 3,938.10^{20}$ sn

- 32 kat dediği için $= \log_2^{(3938,10^{20})} \times 1,5 = 68.416$ yıl gerekli

(18 ay = 1,5 yıl)

...oluşu-

3) 192 bitlik anahtara sahip AES algoritmasını düşünelim. Saniyede $3 \cdot 10^7$ şifre deneyen ASIC (özel entegreler) olduğunu varsayalım. Evrenin tahmin edilen yaşının yaklaşık 10^{10} yıl olduğu kabul edilmektedir. Moore kanununa göre her 1.5 yılda bilgisayarların hızı 2 kat arttığı varsayılmaktadır. Tüm bu bilgiler ve varsayımlar ışığında

a) 100.000 ASIC varsa ve bunlar paralel olarak brute force mantığına göre şifreleri deniyorsa yaklaşık ne kadar sürede anahtar bulunabilir? Bulduğunuz zamanın evrenin yaşına göre karşılaştırınız?

b) A şıkkındaki şartlara göre bu anahtarı tahmin etme hızının 24 saate düşmesi için MOORE kanununa göre kaç yıl geçmesi gerekir?

Cevap:

a) 192 bitlik dediğinde komut sayısı olur.

2^{192} şeklinde alınır

Entegrelerin çarpımı = işlem gücüdür. işlem/sn olur.

$3 \cdot 10^7 \times 10^5 = 3 \cdot 10^{12}$ işlem/sn

$$\rightarrow \frac{2^{192}}{3 \cdot 10^{12}} = 2,092 \cdot 10^{45} \text{ sn}$$

- Ne kadar yıl dediğinde. bulduğun saniyeyi 365.24.60.60'a böleceksin.
(gün, saat, dk, saniye)

$$\rightarrow \frac{2.092 \cdot 10^{45}}{365.24.60.60} = \frac{2.092 \cdot 10^{45}}{3153 \times 10^3} = 6,633 \cdot 10^{37} \text{ yıl sürede anahtar bulunur.}$$

→ Evrenin yaşı dediği 10^{10} soruda verilmiş.

$\frac{\text{Bulduğun yıl}}{10^{10}}$ şeklinde yazacaksın $= \frac{6,633 \cdot 10^{37}}{10^{10}} = 6,633 \cdot 10^{27}$ yıl evrenin yaşı katıdır.

b) Moore kanunları dediğinde moore için verilen değerler alınır.

24 saat demesi $\Rightarrow$ $24 \cdot 60 \cdot 60 = 86400$ sn eder.

$$\frac{\text{komut}}{\frac{\text{komut}}{\text{sn}}} = \text{sn} \longrightarrow \frac{2^{192}}{x} = 86400 \text{ sn}$$

$x = 7,265 \cdot 10^{52}$ komut/sn işlem

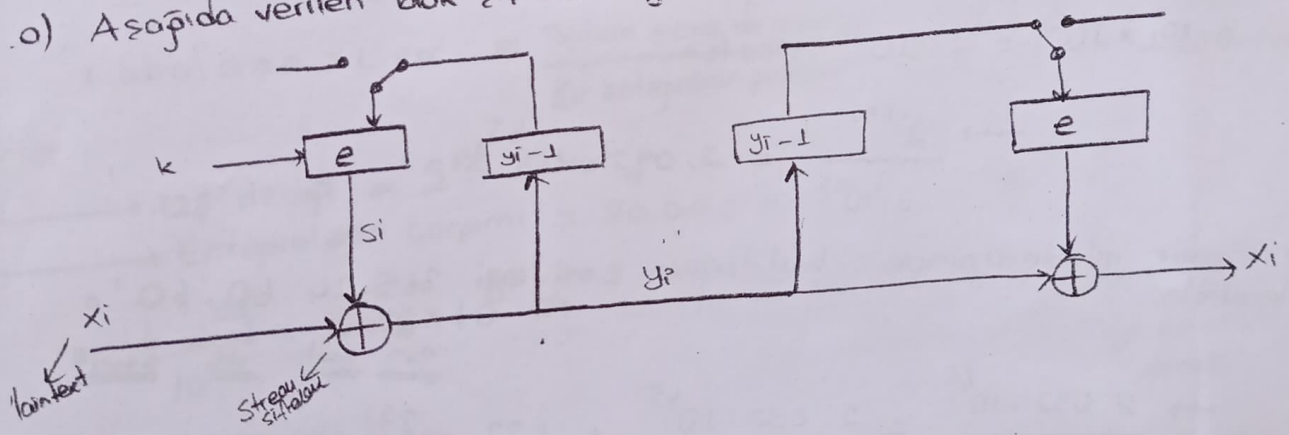
$$\frac{\text{Gerekli işlemci hızı}}{\text{Mevcut işlemci hızı}} = \frac{7,265 \times 10^{52}}{3 \cdot 10^{12}} = 2,421 \times 10^{40} \text{ sn}$$

→ Bilgisayarın hızı 2 kat dediği için → $\log_2$ diye alınır.

→ 10 deseydi → $\log_{10}$ olurdu

$\log_2 (2,421 \times 10^{40}) \times 1,5\,(\text{yıl}) = 201,22$ yıl gerekir.

c) Aşağıda verilen blok şifreleme yöntemi hangi amaç için tasarlanmıştır?



Cevap:

CFB (Cipher Feed Back Mode)

- Asenkron bir akış şifreleme oluşturmak için blok şifrelemeye kullanılır.
- Stream şifrelemeye anahtar üretmek için blok şifreleme kullanılır.