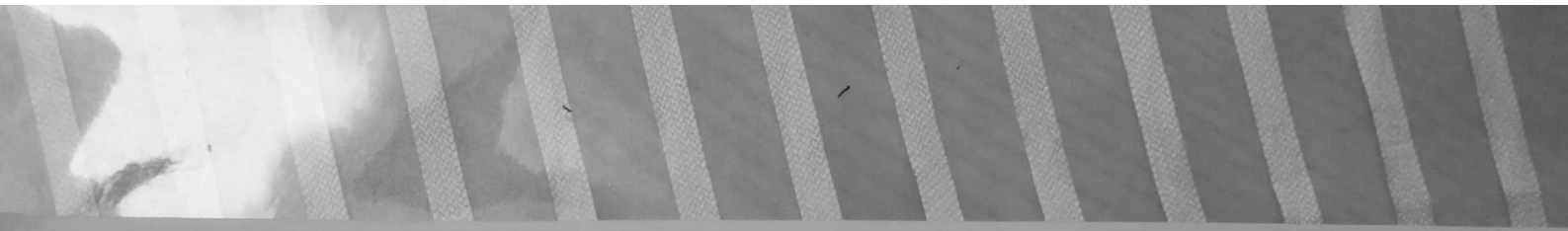

EBRU KARDAŞ
1410161049

Şimdi alacağım bu sınavda dürüstlük ve doğrulukla hareket edeceğime, aşağıdaki sorumluluk ve yükümlülükleri yerine getireceğime söz veririm:

sınav sürecince hiç kimseden yardım almayacağım,

herhangi bir kimse ile sözlü veya yazılı iletişim kurmayacağım,

ekran görüntüleri almayacağım, paylaşmayacağım ve sınav sorularını hiçbir biçimde kopyalamayacağım.

Okudum, anladım, kabul ettim.

Ebru KARDAŞ
1410411008

BİL 470 - Vize

1) a) $C = E([a,b],p) = (a \cdot p + b) \bmod 26$ sezar şifreleyici

$E(k,p) \neq E(k,q)$ (1-1)

Euclid Algoritması

$a = c \cdot q_1 + r_1 \quad 0 \leq r_1 < c \rightarrow a \bmod c = r_1$

$b = c \cdot q_2 + r_2 \quad 0 \leq c < c \rightarrow b \bmod c = r_2$

$(a+b) \bmod c = (c \cdot q_1 + r_1 + c \cdot q_2 + r_2) \bmod c$

$= (c(q_1+q_2) + r_1 + r_2) \bmod c$

Mod c alacağımız için şu kalır:

$(a+b) \bmod c = (r_1 + r_2) \bmod c$

$(a \bmod c + b \bmod c) \bmod c = (r_1 + r_2) \bmod c$

Ebru KARDAŞ
1410111049

1)

b) $[a \pmod n \times b \pmod n] \bmod n \equiv (a \times b) \bmod n$

$a \times (b+c) = ab + ac$

G sonlu evrenindeki modüler aritmetik işlemlerinden olan çarpma işleminin özelliğidir.

→ e, etkisiz eleman olsun

$$e \pmod n \times [a \pmod n \times b \pmod n] =$$

→ Dağılma özelliği kullanılır.

$$[a \pmod n * e \pmod n] \times [b \pmod n \times e \pmod n]$$

$$= (a \times b) \bmod n$$

Esra KAYDAŞ
1411044049

2)a) Bir blok şifreleyici bir özet fonksiyonu ve hatta bir mesaj doğrulama kodu (MAC) oluşturma mümkündür. En kolay yol, giriş verilerinizi CBC gibi blok zincirleme modunda önceden seçilmiş bir anahtarla şifrelenek ve şifrenin son çıktı bloğunu özet (hash) olarak kullanmaktadır.

Ebru [illegible]
1U10444049

2)

b) Feistel Şifreleyicinin parametreleri:

- Blok uzunluğu: Büyük blok uzunluğu daha fazla güvenlik anlamındadır. Fakat şifreleme/desifreleme hızını azaltır. Genelde 64 bitlik bloklar kullanılır.
- Anahtar uzunluğu: Büyük anahtar uzunluğu daha fazla güvenlik anlamındadır. Fakat şifreleme/desifreleme hızını azaltır. Genelde ~~128~~ bitlik anahtar kullanılır.
- Tur sayısı: Daha fazla tur sayısı güvenliği arttırır. Genelde 16 tur kullanılır.
- Ana anahtar üretme algoritması: Karmaşıklığı fazla olan bir alt anahtar üretimi kriptoanalizi zorlaştırır.
- Tur fonksiyonu: fazla karmaşık olan tur fonksiyonu kriptoanalizi zorlaştırır.

Diğer özellikleri:

Analiz kolaylığı: Algoritmanın kriptoanaliz saldırılarına karşı karmaşık olması istense de anlaşılabilirliği azaltır. Örneğin DES anlaşılması güç bir algoritmadır.

Hızlı Yazılım Şifreleme/Desifreleme:

95 ASCII karakter kümesi, Anahtar uzunluğu: 10 karakter

Şifre kırıcının hızı: $6{,}4$ milyon/sn

tüm olası şifrelerin test edilmesi ne kadar zaman alır?

$$t = \frac{95^{10}}{6{,}4 \cdot 10^{6}}$$