Ebru KARDAŞ
1410040049

3) a) DES ve AES özellikleri:

i) f fonksiyonu çıkışının sol yarım ile XOR işlemi

ii) f fonksiyonu:

DES'teki f fonksiyonu, AES'te her turda işleme tabi tutulan (word) kelimelere denk gelir. w[i]

iii) P permütasyonu

DES'teki S-Box (yerine koyma) işleminden sonra elde edilen 32 bitlik çıktı P-Box'ta uygun bir şekilde değiştirilir. Bu değişiklikte girdi pozisyonuna göre çıktı pozisyonu tasarlanır. AES'te Shift-Rows işlemi (basit bir (bayt)ların grup ve sütunlar arasında değiştirme) permütasyonu yapılır.

b) p asal sayı, $x^2 \equiv 1 \bmod p \Rightarrow x \equiv 1 \bmod p$ ve $x \equiv -1 \bmod p$ } ispatla

Halka $(\mathbb{Z}, p, +, \times)$ sonlu alandır ve integral domain'dir.

$x^2 = 1 \Rightarrow (x-1)(x+1) = 0 \Rightarrow ((x-1)=0) \vee ((x+1)=0)$

$x = \pm 1$

CamScanner ile tarandı

Eğm KARDAŞ
1410111019

4)

a) RSA , $n = p \cdot q$, e → açık anahtar

$ebob(\phi(n), e) = 1$ olmalı $\quad d = e^{-1} \bmod \phi(n), \quad 0 \le d \le n$ (yok)

Açık anahtar = $\{e, n\}$

Gizli anahtar = $\{d, n\}$

$C = P^e \bmod n \qquad P = C^d \bmod n$

e, açık anahtar ve n, ortak çarpan verilmesi durumunda

eğer gizli anahtarı hesaplama imkanımız varsa;

$d = e^{-1} \bmod \phi(n), \quad 0 \le d \le n$

verilenlerden d, gizli anahtarı bulunur ve

$P = C^d \bmod d$ denkleminde desifreleme yapılır.

b) EBOB(m,n) = 1 → $\phi(m,n) = \phi(m) * \phi(n)$

Euler - Fermat Teoremi

$m^{\phi(n)} \equiv 1 \bmod n \qquad n^{\phi(n)} \equiv 0 \bmod n$

$m^{\phi(n)} + n^{\phi(n)} = 1 + 0 \bmod n$

$m^{\phi(n)} + n^{\phi(n)} \equiv 1 + 0 \bmod m$

Chinese Kalan Teoreminden

CamScanner ile tarandı

Ebru KAROL
1410110409

4)c) Kriptanaliz: Kriptanalitik saldırılar, algoritmanın özelliği, şifresiz metnin genel karakteristiği hakkında bilgilere ve şifresiz metin-şifreli metin çiftinin bazı örneklerine dayanır. Bu saldırı sonucunda kullanılan anahtar veya şifresiz metin, algoritmanın eksiklerine dayanarak elde edilmeye çalışılır.

Diferansiyel (fark) Kriptanaliz: Şifreli metin çiftleri ile onlara ait şifresiz metin çiftleri arasındaki kısmi farkları araştırır. Bu yöntem, aynı anahtar ile şifrelenen şifresiz metin, DES'in turlarında ilerlerken farkının değişimini analiz eder. En iyi saldırı 2^{47} şifresiz metin veya 2^{55} şifreli metin ve 2^{47} DES işlemi gerektirir.

Doğrusal (Lineer) Kriptanaliz: DES için 2^{47} şifresiz metin ile aynı miktarda şifreli metin karşılaştırılarak anahtar bulunur. Eğer şifresiz metin bloğunun bitlerine birbiri ile XOR işlemi uygulanır, şifreli metin bloğunun bitlerini de bir biri ile XOR'lar ve sonuçlar da XOR'lanırsa anahtar bitlerinin bazılarının XOR'lanarak elde edildiği tek bir bitlik sonuç elde edilir. Bu doğrusal bir yaklaşımdır ve p olasılığı ile sağlanır. $p \neq 0,5$ ise anahtar için kullanılabilir.

Yan Kanal Kriptanalizi!

CamScanner ile tarandı