BİL 438 Bahar 2009– 1. Arasınav **Öğr. No:**

20.03.2009,Ahmet Burak Can **Ad Soyad:**

Soru 1. Block cipher algoritmalarının ECB, CBC, OFB, CFB ve CTR kullanım modlarıyla ilgili olarak aşağıdaki soruları cevaplayınız. (20 puan)

a) …… modları *randomized encryption* özelliği taşır.

b) …… modlarında, şifreleme işlemi sıradüzensel (sequential) yapılmak zorundadır.

c) …… modlarında şifreleme işlemi, bir önişleme (preprocessing) aşamasına ihtiyaç duyulmadan, paralel yapılabilir.

d) …… modlarında, şifreleme sırasında kullanılacak anahtar dizisi önceden üretilerek şifreleme işlemi hızlandırılabilir.

e) …… modu, bütün blokları aynı anahtarla şifrelediği için, disk şifrelemede kullanılabilir. Fakat, bu modda aynı içeriğe sahip iki plaintext aynı ciphertext'e dönüştüğü için, bu mod yerine, her bloğu şifrelemek için ayrı anahtar kullanan ve rastgele seçilen bir blok için anahtarı diğer bloklardan bağımsız olarak üretme imkanı veren, …… modunun disk şifrelemede kullanılması daha uygundur.

Soru 2. Double-DES algoritması 56*2=112 bit anahtar kullandığı halde, meet-in-the-middle saldırısı ile Single DES algoritmasına yakın bir zorlukta kırılabilir. Bu saldırının nasıl yapıldığını ve niçin 112 bitlik anahtar uzayı kullanmasına rağmen yeterince koruma sağlayamadığını anlatınız. (10 puan)

Soru 3. Feistel ağı kullanan bir şifreleme algoritmasında, şifreleme (encryption) işlemleri sırasında, herbir adımda (round) yapılan işlemler, matematiksel olarak aşağıdaki şekilde ifade edilmektedir (L_i: i. adımda sol yarıdaki bitler, R_i: i. adımdaki sağ yarıdaki bitler):

$L_1=R_0 \quad R_1=L_0 \oplus f_1(R_0)$

$L_2=R_1 \quad R_2=L_1 \oplus f_2(R_1)$

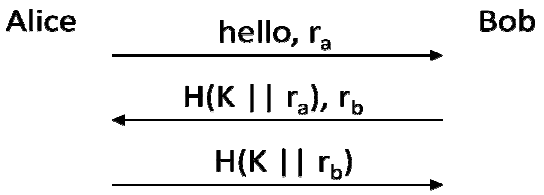
…

$L_d=R_{d-1} \quad R_d=L_{d-1} \oplus f_d(R_{d-1})$

Buna göre, şifrelenmiş bir metnin çözülmesi (decryption) işlemi sırasında herbir adımda yapılması gerekenleri yukarıdaki gibi matematiksel ifadelerle gösteriniz. (7 puan)

Soru 4. One-Time-Pad algoritmasının perfect secrecy sağlamasının nedenleri nelerdir? (10 puan)

Soru 5. Birthday paradox probleminden yola çıkarak bir hash işlevinin tasarımında dikkat edilmesi gereken önemli kriteri açıklayınız. (10 puan)



Soru 6. Alice ve Bob, birbirlerinin kimliklerini doğrulayabilmek (authenticate) için, yukarıdaki çizimde verilen protokolü kullanmaktadır. Bu protokolü çalıştırmadan önce, K anahtarının sadece Alice ve Bob tarafından bilindiği varsayılmaktadır. r_a ve r_b , sırayla Alice ve Bob tarafından rastgele seçilmiş sayılardır. Bu protokolü, hash işlevi yerine bir simetrik şifreleme algoritmasıyla gerçekleştirebilmek için nasıl değiştirmek gerektiğini (yukarıdaki gibi bir çizimle) gösteriniz. Çizim üzerinde kullandığınız kısaltmaları açıklamayı unutmayınız. (10 puan)

Soru 7. Aşağıdaki beş kavramı birer cümleyle açıklayınız. (10 puan)

Digital signature:

Digital certificate:

Certificate Authority:

Stenography:

Non-repudiation:

- p, q, büyük asal sayılarını seç
    - n = pq ve $\varphi(n) = (q-1)(p-1)$ değerlerini hesapla
- gcd(e, $\varphi(n)$) = 1 değerini sağlayan bir e sayısı seç.
- $ed \equiv 1 \bmod \varphi(n)$, denkliğini sağlayan bir d değeri hesapla.

Soru 8. Yukarıda, RSA algoritmasındaki parametrelerin hesaplanışı verilmiştir. RSA algoritmasıyla ilgili aşağıdaki soruları cevaplayınız. (15 puan)

a) Public key: ……..
Private key: ……..
Encryption:……..
Decryption:……..
şeklinde olmalıdır.

b) Decryption işleminde, ciphertext'den nasıl plaintext elde edildiğini, Euler'in teoremini dikkate alarak, matematiksel olarak gösteriniz. (Euler teoremi: $a^{\varphi(n)} \equiv 1 \pmod n$, if n>1, gcd(a,n)=1)

c) RSA algoritmasını kırmanın güçlüğü hangi probleme dayanmaktadır? Bir saldırgan, hangi parametreleri bulursa algoritmayı kırabilir?

Soru 9. $MAC_K(x) = H(K \,||\, x)$ şeklinde üretilen bir message authentication code üzerinde yapılabilecek bir saldırıyı anlatınız. Bunu çözmek için $MAC_K(x)$ işlemi nasıl değiştirilebilir? (8 puan)