ANKARA ÜNİVERSİTESİ – BİLGİSAYAR MÜHENDİSLİĞİ

08.06.2023

BLM 426 & 4530 Bilgi Güvenliği
Final Sınavı
Süre: 75 dk.

ID: **Ad Soyad:** **İmza:**

1. (5). Aşağıdakilerden hangisi DES tarafından desteklenen kabul edilebilir bir anahtar uzunluğudur? (Which one of the following is an acceptable key length supported by DES?)

a) 32 bits
b) 56 bits
c) 128 bits
d) 192 bits

2. (5). AES'de kullanılan blok boyutu nedir? (What is the block size used in AES?)

a) 128 bits
b) 192 bits
c) 256 bits
d) 128 or 192 or 256 bits

3. (5). Aşağıdakilerden hangisi bir özet fonksiyonudur? (Which of the following is a hash function?)

I. MD5
II. SHA-1
III. RSA

a) Yalnız I
b) Yalnız II
c) I ve II
d) II ve III

4. (5). Aşağıdakilerden hangisi bir simetrik şifreleme yöntemidir? (Which of the following is a symmetric encryption method?)

I. RSA
II. DES
III. AES

a) Yalnız I
b) Yalnız II
c) I ve II
d) II ve III

5. (5). Aşağıdakilerden hangisi bir asimetrik şifreleme yöntemidir? (Which of the following is a asymmetric encryption method?)

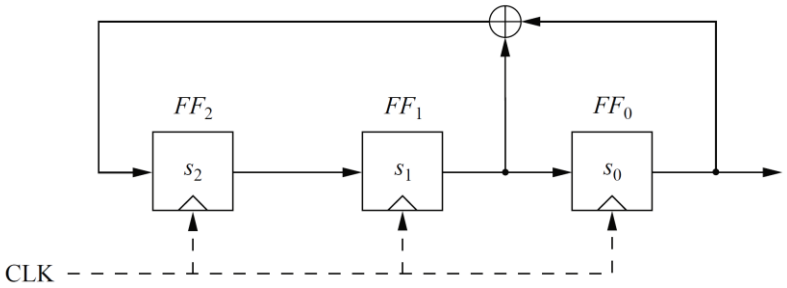
I. RSA
II. DES
III. AES

a) Yalnız I
b) Yalnız II
c) I ve II
d) II ve III

6. (15). Dijital imzalar ile hangi güvenlik hizmetleri sağlanabilir? (Which security services can be provided by digital signatures?)

---

7. (20). Verilen LFSR yapısını ve başlangıç değerlerini kullanarak ilk bayt (8 bit) çıktıyı hesap ediniz. (Calculate the first byte (8 bits) output using the given LFSR structure and initial values.)



CLK	FF_2	FF_1	$FF_0 = s_i$
0	0	0	1
1			
2			
3			
4			
5			
6			
7			

---

8. (20). Anahtarları (n = 33, e = 3) olan bir RSA imza şeması verildiğinde, aşağıdaki imzalardan hangisi geçerlidir? (Given an RSA signature scheme with the keys (n = 33, e = 3), which of the following signatures are valid?)

a) x = 5, sig(x) = 12

b) x = 5, sig(x) = 14

---

9. (20). "(3, 1) + (5, 1)" işlemini $y^2 \equiv x^3+2x+2 \bmod 17$ eğrisi üzerinde uygulayın. (Perform the addition "(3, 1) + (5, 1)" in the group of the curve $y^2 \equiv x^3+2x+2 \bmod 17$)