ANKARA ÜNİVERSİTESİ – BİLGİSAYAR MÜHENDİSLİĞİ

27.04.2023

BLM 426 & 4530 Bilgi Güvenliği
Ara Sınavı
Süre: 120 dk.

ID: **Ad Soyad:** **İmza:**

1. (15). Diffie–Hellman anahtar değişimi protokolüne göre p = 73, α = 3, a=5 ve b=7 seçilmesi durumunda ortak anahtarı hesap edin.

2. (15). GF(2^8)'de (x^7+ x^5+x^3+x) * (x^5+ x^3+x^2+x) mod P(x) işleminin sonucu nedir? (P(x) = x^8+x^4+x^3+x+1)

3. (15). Ali ve Bülent tek seferlik pad (One Time Pad) şifreleme sistemini kullanıyor. Açık metnin "1010 1010 1010" ve şifreli metnin "1111 1111 0000" olduğunu varsayalım. Bu durumda metni şifrelemek için kullanılan anahtar nedir?

4. (20). 13 sayısının mod 37 çarpmaya göre tersini Extended Euclidean yöntemi kullanarak hesap edin

5. (15). Girdinin "111000" olması durumunda S5 tablosuna göre çıktı ne olmalıdır?

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

6. (20). Square-and-multiply algoritmasını uygulayarak "2^{43} mod 97" sonucunu hesaplayın.