Ad-Soyad :
Numara :

06.11.2017

İNFORMASYON GÜVENLİĞİ VE KRİPTOLOJİ VİZE SINAVI

1-) **a)** $x^{38} \equiv 3 \pmod{13}$ denkleminin çözüm kümesini Fermat Teoreminden yararlanarak bulun. **(5p)**

b) 123^{562} sayısının son 2 dijiti(rakamı) nedir? **(5p)**

c) Fibonacci sayılarda(1, 1, 2, 3, 5, 8, ….) $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ ise Euclid Algroritmasına göre $\gcd(F_n, F_{n-1})$ değerini tüm $n > 1$ içi hesaplayın. **(10p)**

2-)

a) $7d \equiv 1 \pmod{30}$ ise d=? **(5p)**

b) $x^2 \equiv 77 \pmod{143}$ ise x'in çözüm kümesini bulun. **(5p)**

c) Geçit töreni için hazırlanan bir grupta sıralar 3'erli dizildiği zaman 1 kişi, 4'erli dizildiği zaman 2 kişi, 5'erli dizildiği zaman 3 kişi açıkta kalıyor. Bu grupta bulunan minimum kişi sayısı kaçtır? **(10p)**

3-)

a) Z_{88}'de Affine Cipher yöntemi için anahtar uzayı boyutu nedir? **(10p)**

b) mod 26 uzayında arka arkaya 2 defa Affine Cipher kullanıldığında tek bir defa Affine Cipher kullanılmasına karşın avantajlı olup olmadığını açıklayın. **(5p)**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

4-)

a) Hill Cipher'da mod 26 uzayında Anahtar Matris $\begin{pmatrix} 1 & 1 \\ b & 1 \end{pmatrix}$ ise b'nin alabileceği değerleri hesaplayın? **(5p)**

b) Hill Cipher'da mod 26 uzayında $\begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix}$ matrisi kullanılarak ciphertext: "IBUXZH" ise plaintext? **(10p)**

5-) (Bu soru soru kağıdı üzerinde cevaplanacaktır!!!)

a) Feistel Şifrelemede herbir şifreleme döngüsünde $L_i = R_{i-1}$ ise R_i=? **(5p)**

b) 3K(3-DES) için kullanılan anahtar uzunluğundan kontrol bitlerini çıkardığımızda uzunluk kaç bittir? **(5p)**

c) DES işlem kiplerinden CBC işlem kipinde sadece y_i bloğu bozulduğunu(hatalı iletildiğide) ve diğer blokların düzgün bir şekilde iletildiğini varsayalım. Bu durumda şifre çözülürken düzgün bir şekilde çözülemeyen blok/bloklar var mıdır ve varsa hagisi/hangileridir?**(10p)**

d) Brute Force anahtar arama yöntemi kullanılarak 3 anahtarlı 3-DES anahtarı 2 anahtarlı 3-DES'e nazaran kırılması ne kadar daha fazla zaman alır? **(10p)**

Başarılar…

Sınav Süresi :70 dk.