

Ad-Soyad :
Numara :

05.11.2018

İNFORMASYON GÜVENLİĞİ VE KRİPTOLOJİ VİZE SINAVI

- 1-) a) p asal olsun, $a^{\phi(p)} \equiv 1 \pmod{p}$ olduğunu gösterin. (5p)
b) 2^{1000} ün 101'e bölümünden kalan kaçtır? (5p)
c) Euler $\phi(n)$ fonksiyonu nedir? Euler $\phi(132)=?$ (5p)
- 2-) a) $4^x \pmod{7}$ ve $4^y \pmod{20}$ işlemlerini Cebirin Temel Teoremi'ne göre bulun. (10p)
b) $17x + 101y = d$ denklemindeki x, y ve d değerlerini bulun. $17^{-1} \pmod{101}=?$ (10p)
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 açığa kalıyor. Bu grupta bulunan minimum kişi sayısı kaçtır? (10p)

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

- 3-) a) Z₂₆'de Affine Cipher yöntemi için anahtar uzayı boyutu nedir? (10p)
b) İngiliz alfabesinin ilk 16 harfi kullanılarak bir plaintext Hill Cipher ile $\begin{pmatrix} 3 & 8 \\ 5 & 7 \end{pmatrix}$ matrisi kullanılarak şifreleniyor. Çalışma uzayı Z₂₆! Ciphertext="MCNE" olduğuna göre plaintext'i bulunuz. (10p)

- 4-) Aşağıda Autokey Cipher'in modifiye edilmiş hali verilmiş olsun;

$$y_i = (x_i + K) \pmod{26}, \quad 0 \leq K \leq 25$$

$$y_n = (x_n + y_{n-1}) \pmod{26}, \quad n > 1.$$

Modifiye edilmiş bu hali Autokey Cipher'dan daha güvenli midir? Ciphertext "IMXIW" olduğu durumu gözönünde bulundurarak inceleyiniz. Verilen bu ciphertext'in kırılıp kırılmayacağını gösterin. (10p)

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

- a) $S_8(101001)=?$ (5p)

S₈-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

- b) 2K(3-DES) için kullanılan anahtar uzunluğundan kontrol bitlerini çıkardığımızda uzunluk kaç bittir? (5p)

- c) Feistel Şifrelemede her bir şifreleme döngüsünde $L_i = R_{i-1}$ ise $R_i = ?$ (5p)

- 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.