11.11.2021

İNFORMASYON GÜVENLİĞİ VE KRİPTOLOJİ ARA SINAV SORULARI

1-) a) p asal olsun. $a^p \equiv a \pmod p$ olduğunu gösterin. **(5p)**

b) 2^{10203} ün 101'e bölümünden kalan kaçtır? **(5p)**

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

d) Euler phi(Ø) fonksiyon nedir? Euler Ø(88)=? **(5p)**

2-)

a) $4^{-1} \pmod 7 = ?$ $4^{-1} \pmod{20} = ?$ İşlem sonuçlarını Cebirin Temel Teoremine göre bulun. **(5p)**

b) $17x + 101y = d$ denklemindeki x,y ve d değerlerini bulun. $17^{-1} \pmod{101} = ?$. **(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? (Çinli Kalanlar Teoremine göre bulunacak) **(10p)**

3-)

a) Z_{88}'de Affine Cipher yöntemi için anahtar uzayı boyutu nedir? **(5p)**

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

c) İngiliz alfabesinin ilk 16 harfi kullanılarak bir plaintext Hill Cipher ile $\begin{pmatrix} 3 & 8 \\ 5 & 7 \end{pmatrix}$ matrisi kullanılarak şifreleniyor. Çalışma uzayı Z_{16}! Ciphertext= "MCNE" olduğuna göre plaintext'i bulunuz. **(10p)**

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

$y_1 = (x_1 + K) \bmod 26, \quad 0 \le K \le 25$

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

Modifiye edilmiş bu hali Autokey Cipher'dan daha güvenli midir? Ciphertext "IMXIW" olduğu durumu gözönünde bulundurarak inceleyiniz. Verilen bu ciphertext'in kırılıp kıralamayacağını gösterin. **(20p)**

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

5-) **(Soru Kağıdı üzerine cevaplanacaktır!)**

a) 2 anahtarlı (3-DES) için kullanılan anahtar uzunluğundan kontrol bitlerini çıkardığımızda uzunluk kaç bittir? **(5p)**

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

c) $S_6(101001) = ?$ **(5p)**

S_6-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

Sınav Süresi :70 dk., Başarılar