DENEY-2 SORULAR
SON TESLİM TARİHİ: 25/10/2019 CUMA GÜNÜ SAAT 13:55

S.1 C=(p+k)(mod 26) bağıntısıyla yapılan şifreleme yönteminin bilinen adı nedir? Bu yöntemde şifreli metinden düz metine geçiş için hangi özdeşlik kullanılır?

S.2 Vigenere şifreleme ile kaydırma şifrelemesi arasındaki fark nedir? Hangisi ile yaratılmış şifreli metni çözmek daha kolaydır? Açıklayınız.

S.3 Aşağıdaki tabloyu kullanarak Ad ve Soyadınızı k1=(21,4,2,19,14,17) ve k2= (9,5,14,14,17) enkripsiyon anahtarları ile şifreleyiniz? (Şifrelenecek metni küçük harflerle, şifrelenmiş metni büyük harfler ile gösteriniz.)

a	b	c	ç	d	e	f	g	ğ	h	ı	i	j	k	l	m	n	o	ö	p	r	s	ş	t	u	ü	v	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	26	27	28
A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z

S.4 Karakterlerin sıklık bilgisi kullanılarak Vigenere Şifrelemenin nasıl kurulabileceğini açıklayınız.

S.5 Vigerene şifreleme ile şifrelenmiş bir Türkçe metnin çözülebilmesi için ihtiyaç duyulan aşağıdaki harf frekans tablosu için gereken verileri temin ediniz.

a	b	c	ç	d	e	f	g	ğ	h
ı	i	j	k	l	m	n	o	ö	p
r	s	ş	t	u	ü	v	y	z	

S.6 Vigerene şifreleme yöntemi ile şifrelenmiş bir metin veriliyor. Bu şifrelemede kullanılan anahtarın boyunun 5 olduğu biliniyor. Anahtarın 1. karakterini oluşturan harfi bulabilmek için 1.,6.,11.,16., …v.s. konumlarında bulunan karakterlerin sıklıkları alfabetik sıraya sokulduktan sonra aşağıdaki sıklık vektörü (**V vektörü**), bulunmuştur. Bağıl sıklık vektörünü (**w vektörü**) elde ediniz.

V = (0,0,7,1,1,2,9,0,1,8,8,0,0,3,0,4,5,2,0,3,6,5,1,0,1,0) ➔ W = ?

A_0 = (.082, .015, .028, .043, .127, .022, .020, .061, .070, .002, .008, .040, .024, .067, .075, .019, .001, .060, .063, .091, .028, .010, .023, .001, .020, .001)

Her bir **$W.A_i$** skaler çarpım sonucunu **$0 \le i \le 25$** için hesaplayınız. En büyük **$W.A_i$** skaler çarpım değerine karşılık gelen karakter hangisidir?