TOBB Ekonomi ve Teknoloji Üniversitesi - Matematik Bölümü
2014-2015 Bahar Dönemi - MAT 421-515 Şifreleme Bilimine Giriş
ARA SINAVI

Ad-Soyad: **No:** **İMZA:**

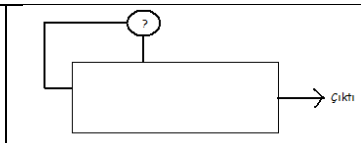
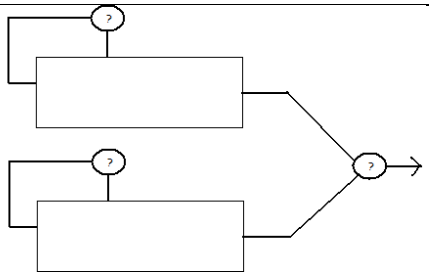
12.03.2015

Başarılar

1. **(10 puan)** İngiliz alfabesini kullanarak dört harfi dört harfe götüren **basit** bir şifreleme sistemi tasarlayınız.
   - **a.** Şifreleme ve deşifreleme yönteminizi algoritmik olarak adım adım yazınız.
   - **b.** Sisteminizdeki geçerli anahtar sayısını belirtiniz.
   - **c.** FBSS GSTS BJKX metnini şifreleyiniz (Anahtar: Öğrenci numaranızın veya isminizin uygun bir kısmını kullanınız.)
   - **d.** c. şıkkında elde ettiğiniz şifreli metni deşifre yönteminizi kullanarak doğrulayınız.
2. **(15 puan)** Aşağıdaki İngilizce metnin anlamlı olduğu ve Afin şifreleme sistemi ile şifrelendiği bilinmektedir. Açık metni ve şifreleme anahtarlarını bulunuz. Cevabınızın detaylarını açıklayınız.

FMXVE DKAPH FERBN DKRXR SREFM ORUDS DKDVS HVUFE DKAPR KDLYE VLRHH RH

3. **(20 puan)** $f_1(x_1, x_2, x_3, x_4) = x_4 + x_1$, $f_2(x_1, x_2, x_3) = x_1 + x_3$ ve $f_3(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$ fonksiyonları kullanılarak aşağıdaki kısıtlara uygun bir akan şife sistemi tasarlanmak istenmektedir.

a.	Bağlantı polinomu olarak f_1, f_2, f_3 den hangisini seçilirse LFSR ın periyodu maksimum olur? Neden?	
b.	f_1, f_2, f_3 polinomlarını birden fazla kullanma imkanı olduğunda aşağıdaki sistemin periyodunu maksimum yapmak için "?" olan yerlere hangi fonksiyonlar yerleştirilmelidir? Bu durumda sistemin periyodu ne olur? Bu sistemin çıktısı ile "isminiz ve soy isminizden" oluşan açık metni şifreleyiniz. Seçtiğiniz anahtarı belirtiniz.	

4. **(15 puan)** F_2^8 den F_2 ye tanımlı f fonksiyonunun *Walsh değerleri* $W_f(a)$ ile gösterilmek üzere, tüm Walsh değerlerinin karelerinin toplamının, $\sum_{a \in F_2^8} (W_f(a))^2$, alabileceği **en büyük ve en küçük değerleri** bulunuz.
5. **(10 puan)** $x^{137} = 428 \bmod 541$ ve $y^{751} = 677 \bmod 8023$ denkliklerini sağlayan x ve y değerlerini bulunuz. Çözüm yolunuzun detaylarını açılayınız. (Brute-force kabul edilmez!!! Sadece doğrulama amaçlı kullanılabilir…)
6. **(10 puan)** İngiliz alfabesi ve 2x2 lik matrisler kullanılarak tanımlanan Hill Şifreleme sistemini kısaca açıklayınız. Sistemdeki geçerli anahtar sayısını bulunuz ve nedenini açıklayınız.
7. **(20 puan)** Bir K anahtarı ile şifreleme yapılan bir şifreleme sisteminde $E_K(M) = M$ olacak şekilde şifrelenmiş hali kendisi olan mesajlara sabit mesajlar denir. N=pq olmak üzere, açık anahtarı (N,e) olan bir RSA şifreleme sistemindeki sabit mesaj sayısını p, q ve e cinsinden bulunuz.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001