TÜBİTAK
BİLGEM
BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Haziran Ayının Ödüllü Soru ve Cevapları

Soru 1 :

Dizi şifreleme (stream cipher) algoritmalarında, açık yazı bloklar halinde değil de, daha küçük seviyelerde (örneğin, bit ve baytlar) işlenmekte, ve genelde, gizli bir anahtara bağımlı olarak üretilen sözde rastgele bit dizileri ile XOR işlemi, gizli yazıyı oluşturmaktadır. Yani, A: işlenecek açık yazı ünitesi, K: anahtara bağlı sözde rastgele bit dizisi, ve G: çıktı olan gizli yazı ünitesi olmak üzere, $A \oplus K = G$ olmaktadır. Bu durumda, aşağıdaki tabloda boş bırakılan yerlere hangi 8-bitlik üniteler gelmelidir?

Açık Ünite	***Anahtar dizisi***	***Gizli Ünite***
10110100	00101101	?
01100010	?	11010011
?	01011100	01110110

Cevap 1 :

10011001
10110001
00101010

XOR işlemi, ve $A \oplus K = G$ nin özelliklerinden, şu eşitliklere ulaşabiliriz:

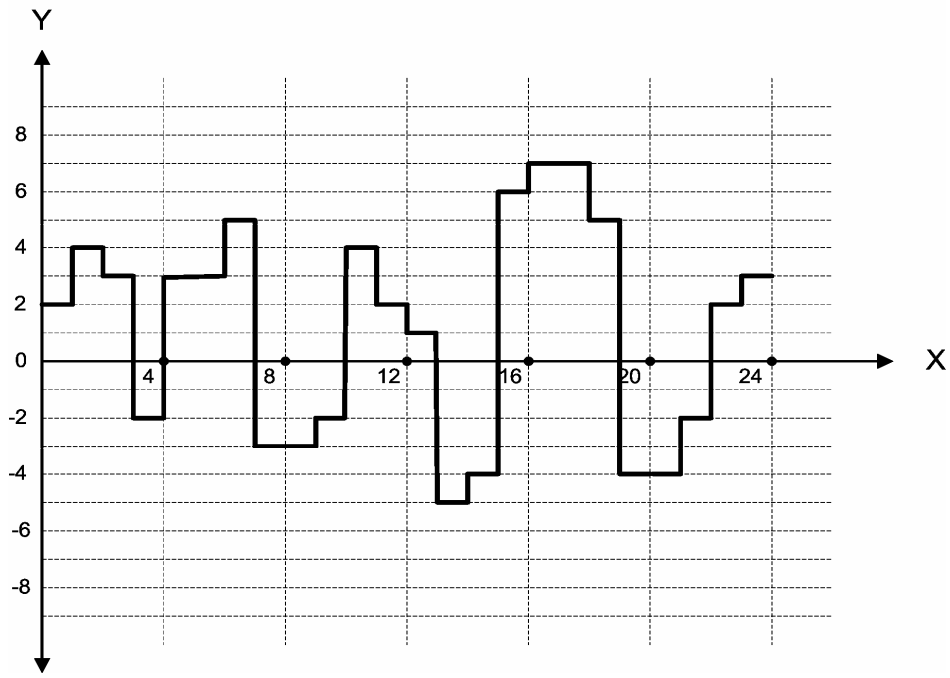
$G \oplus K = A$ ve $A \oplus G = K$

Yani, A, G, ve K üçlüsünden herhangi ikisi verildiğinde, sorulan değeri bulmak için, verilen iki diziyi XOR işleminden geçirmek yeterlidir. Bu durumda,

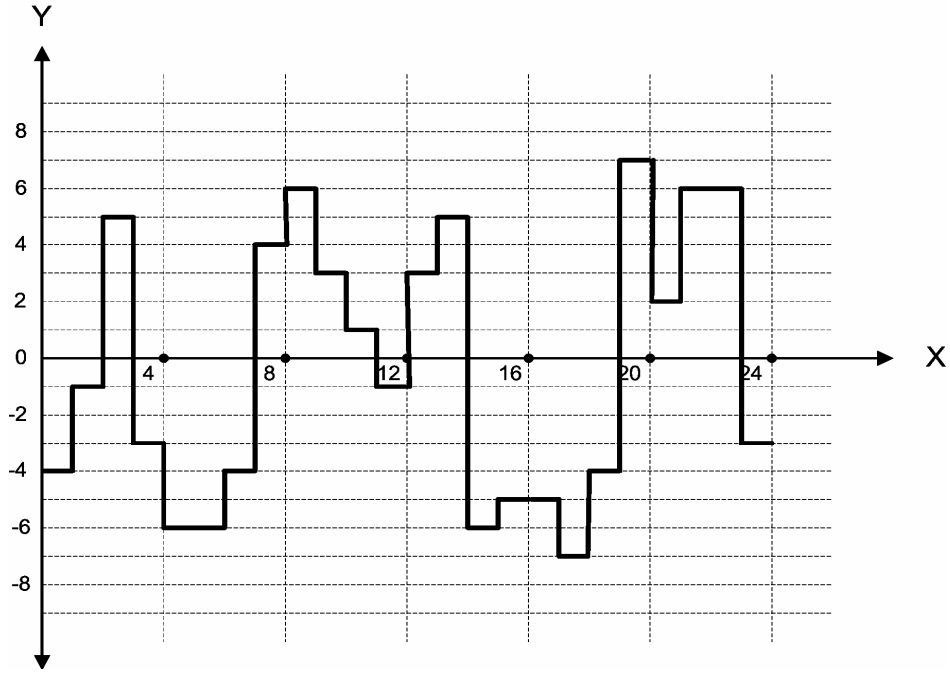
Satır 1: $A \oplus K = G$ → G = 10011001
Satır 2: $A \oplus G = K$ → K = 10110001
Satır 3: $G \oplus K = A$ → A = 00101010

olmaktadır.

Soru 2 :



→ İLİNTİ



→ ?

Cevap 2 :

KRİPTO

Verilen sinyal değerleri kümesinde, X eksenindeki her 4 birimlik kısım, sırasıyla bir açık yazı harfini kodlamaktadır: bu kısımdaki sinyalin toplam gücü (X ekseninin altında ve üstünde bulunan sinyal alanı toplamı), alfabemizdeki harflerin sıra değerlerini (A = 0, B = 1, …, Z = 28) yansıtmaktadır.

Yani:

1. harf → X = [0,4] → sinyal alanı toplamı = 9 + 2 = 11 → harf = İ

2. harf → X = [4,8] → sinyal alanı toplamı = 11 + 3 = 14 → harf = L

3. harf → X = [8,12] → sinyal alanı toplamı = 5 + 6 = 11 → harf = İ

…

Aynı kural, ikinci sinyale uygulanırsa:

1. harf → X = [0,4] → sinyal alanı toplamı = 5 + 5 + 3 = 13 → harf = **K**

2. harf → X = [4,8] → sinyal alanı toplamı = 16 + 4 = 20 → harf = **R**

3. harf → X = [8,12] → sinyal alanı toplamı = 10 + 1 = 11 → harf = **İ**

…

KRİPTO cevabına erişilir.

Soru 3 :

5, 11, 19, 31, 53, 67, 89, 103, 131, 167, ?

Cevap 3 :

181

Dizinin elemanları yazılırken, p_i , i. asal sayı olmak üzere, $p_{(i+p_i)}$, i = 1, 2 , 3 , 4, … kuralıyla bulunan asal sayılar kullanılmıştır.

Yani:

i = 1 → $p_{(1+p_1)} = p_{(1+2)} = p_3 = 5$

i = 2 → $p_{(2+p_2)} = p_{(2+3)} = p_5 = 11$

i = 3 → $p_{(3+p_3)} = p_{(3+5)} = p_8 = 19$

i = 4 → $p_{(4+p_4)} = p_{(4+7)} = p_{11} = 31$

i = 5 → $p_{(5+p_5)} = p_{(5+11)} = p_{16} = 53$

…
…

olmaktadır. Bu durumda, dizinin sorulan 11. elemanı:

i = 11 → $p_{(11+p_{11})} = p_{(11+31)} = p_{42} = 181$

olarak bulunur.