Kriptografi & Steganografi

"POLYBIUS'UN DAMA TAHTASI"

Elemanları harfler olan 5*5 lik bir matristen oluşmaktaydı.

SİSTEM: Alfabe sırayla matrisin sıralarına yazılır ve her harfi belirleyen iki rakam bulunduğu satırı, ikinci rakam bulunduğu sütunu temsil eder.

A=11, B=12

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	R	S	T	U
5	X	W	V	Y	Z

«4442332432244411425 4«

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	R	S	T	U
5	X	W	V	Y	Z

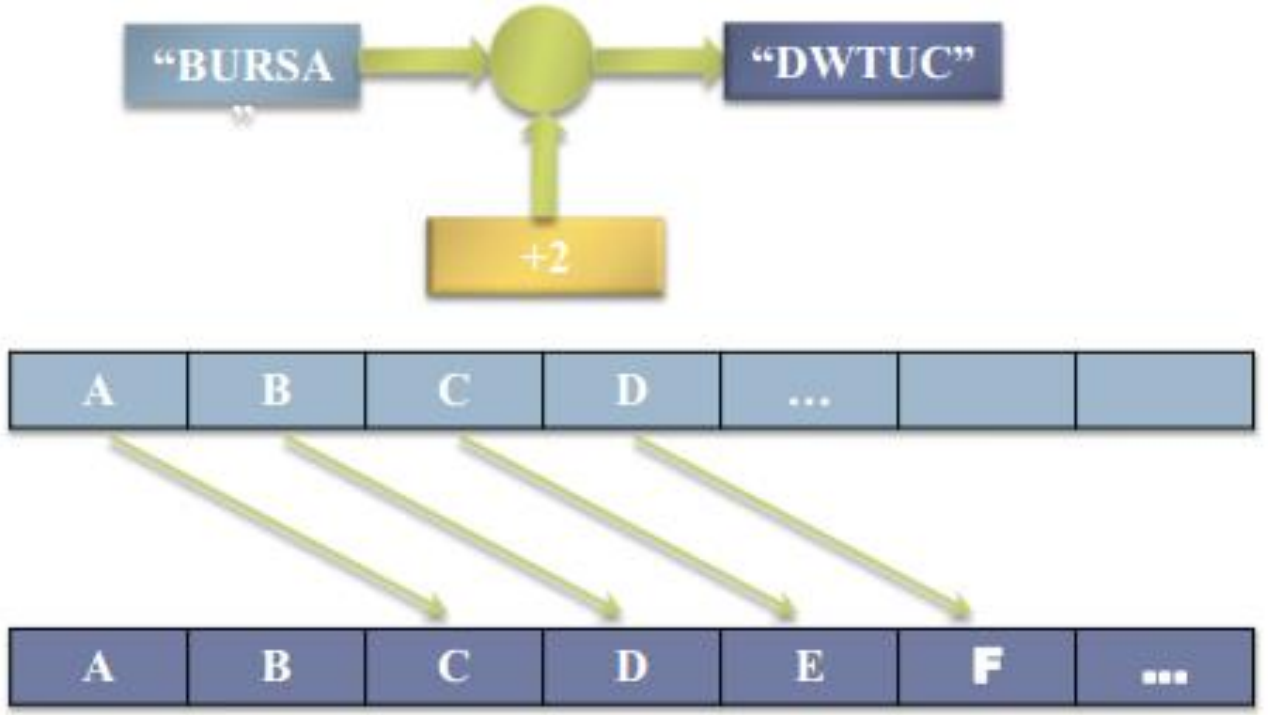
TRMILITARY

Uygulama

Herhangi bir görsel programlama dilinde kodlayınız!

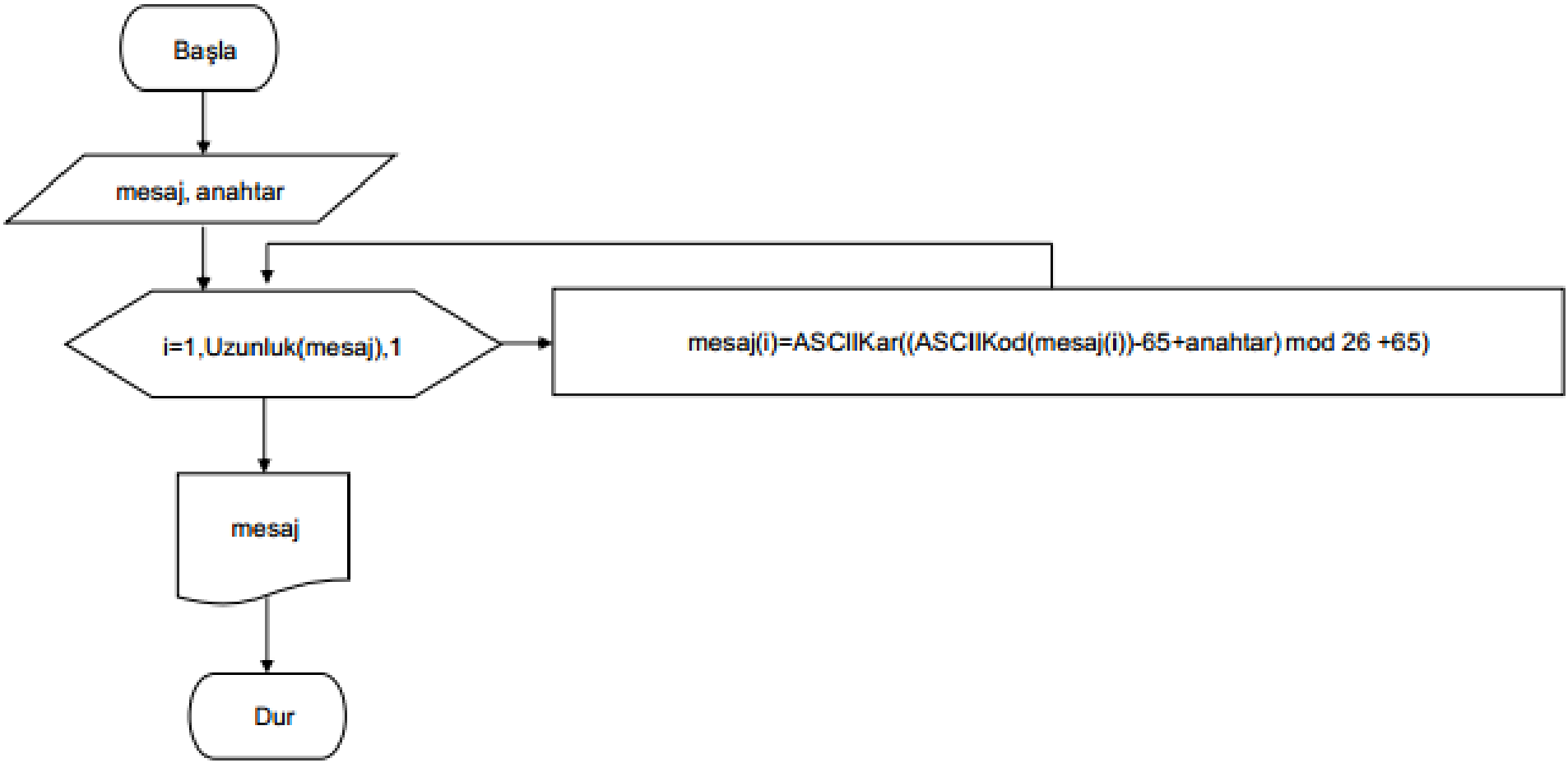
Mesajı yazıldığında kriptosu, kripto yazıldığında mesaj çıkartılabilecek!

Sezar şifreleme



Eğer anahtar değeri 2 ise orijinal mesajdaki her harf, kendisinden iki sonraki harfle yer değiştirir. Yani orijinal mesajdaki "A"→"C", "B"→"D" olur.

Sezar şifreleme algoritması



Uygulama

- Sezar şifreleme algoritmasını bildiğiniz bir dilde kodlayınız!

RSA Algoritması

Yeterince büyük iki adet asal sayı seçilir: Bu sayılar örneğimizde p ve q olsunlar.

$n=pq$

$\varphi(n) = (p-1)(q-1)$

$1 < e < \varphi(n)$

$de \equiv 1 \bmod (\varphi(n))$.

Şifreleme işlemi:

$c = m^e \bmod n$

Şifrenin Açılması:

$m = c^d \bmod n$

Rsa örnek

Örnek:

İki asal sayı seçilir

$p = 61$ ve $q = 53$

n değeri hesaplanır n = pq şeklinde

$n = 61 * 53 = 3233$

Totient fonksiyonu hesaplanır

$\varphi(n) = (p-1)(q-1)$

$\varphi(n) = (61-1)(53-1) = 3120$

totient fonksiyon sonucu ile aralarında asal olan ve 1 den büyük bir sayı seçilir

$e > 1 \Rightarrow e = 17$ (3120 ile aralarında asal) , bu sayı aynı zamanda umumî şifredir.

Hususî şifre olması için bir d sayısı seçilir:

$de \equiv 1 \bmod(n)$ olacak şekilde d sayısı bulunur , $d = 2753$ (çünkü $17 * 2753 = 46801 = 1 + 15 * 3120$) Bu sayının hesaplanması sırasında uzatılmış öklit (extended euclid) yöntemi kullanılmıştır.

Örneğin mesaj olarak 123 gönderilecek olsun:

$123^{17} \bmod 3233 = 855$ olarak şifreli metin bulunur.

açacak taraf için tersi işlem uygulanır:

$855^{2753} \bmod 3233 = 123$ şeklinde orjinal mesaj geri elde edilir.

Araştırma konuları

- Vigenere şifresi
- Vernam şifresi

- Sık kullanılan RSA, DES ve AES, Diffie Hellman algoritmaları kodlayınız. Çalışma mantıklarını kavrayarak birbirlerinden farklılıklarını raporlayınız.

Steganografi – uygulama matlab

```
%kaynak mathworks
clc;
clear all;
close all;
cover = input('Enter cover image: ', 's');
message = input('Enter message image name: ', 's');
x = imread(cover);        % cover message
y = imread(message);    % message image
n = input('Enter the no of LSB bits to be subsituted- ');
S = uint8(bitor(bitand(x,bitcmp(2^n-1,8)),bitshift(y,n-8))); %Stego
E = uint8(bitand(255,bitshift(S,8-n))); %Extracted
origImg = double(y);   %message image
distImg = double(E);   %extracted image
[M N] = size(origImg);
distImg1=imresize(distImg,[M N]);
error = origImg - distImg1;
MSE = sum(sum(error .* error)) / (M * N);
if(MSE > 0)
    PSNR = 10*log10(M*N./MSE);
else
    PSNR = 99;
end
disp('PSNR of message image to extracted image is')
disp(abs(PSNR))
disp('MSE is')
disp(abs(MSE))

figure(1),imshow(x);title('1.Cover image')
figure(2),imshow(y);title('2.Message to be hide')
figure(3),imshow((abs(S)),[]);title('3.Stegnographic image')
figure(4),imshow(real(E),[]); title('4.Extracted image')

figure(5),imhist(x); title('Histogram of cover image')
figure(6),imhist(S); title('Histogram of transformed stego image')
```