ALGORİTMA ÖRNEK ŞİFRELEME VE DEŞİFRE

Algoritmada ikiz asal sayılar **a=13** ve **b=11** ikiz asal sayıları olsun ve **n=10** olsun. İkiz asal sayılar kolay kolay değiştirilmeyecek. Buna göre anahtarlar için "e" ve "d" sayılarını Öklid Algoritması ile bulalım.

$1 \langle e \langle 2^{10}$ olacak şekilde bir "e" sayısı olsun. Öyle ki;

$e.13 \equiv 1 \pmod{2^{10}}$ olsun.
13.e-512.k=1 "k" bir tamsayı
512=13.39 + 5
13=5.2 +3
5=3.1 +2
3=2.1+1 ise 1=3-2.1
1=3-1.(5-3.1)=2.3-1.5
1=2.(13-5.2)-1.5=2.13-5.5
1=2.13-5.(512-13.39)=197.13-5.512
Buna göre **e=197** olur.

$1 \langle d \langle 2^{10}$ olacak şekilde bir "d" sayısı olsun. öyle ki;

$11.d \equiv 1 \pmod{2^{10}}$ olsun.
11.d-m.512=1 " m" bir tamsayı
512=11.46+6
11=6.1+5
6=5.1+1 ise 1=6-1.5
1=6-1.(11-6)=2.6-1.11
1=2.(512-11.46)-1.11=2.512-23.11 buradan d=-11 olur. Negatif olamayacağından 512-11=501 çıkar. Yani **d=501** olur.

Mesaj gönderen kapalı anahtarı

a.b=13.11=143

Mesaj alıcının kapalı anahtarı

e.d=197.501=98697

Gözlem anahtarı

$2^{n-1}=2^9$

Gönderilecek karakter "A" olsun. CBKİHA Karakter Kodu

"133"

Açık anahtar

$m^{a.b}=133^{143}$

$$13^{2^9} - 11^{2^9} \equiv 0 \pmod{2^{10}}$$

“a=13” ve “b=11” ikiz asal sayı, n=10

Mesaj göndericinin orjinal mesaj kodu

“m=133”

CBKİHA Karakter Tablosunda “A”

Gönderici kapalı anahtarı

”a.b=143”

Mesaj gönderenin kapalı anahtarı ile şifrelenmiş mesaj:

“133^{143}”

Herkes

Görebilir.

Açık anahtar olarak herkesin görebileceği şifreler

(133^{143})

Mesaj alıcının kapalı anahtarı “ d.e=98697”

Şifreli mesajı açmaya çalışan mesaj alıcının kapalı anahtarı ile oluşan şifreli mesaj

$133^{(14113671)} \equiv x \pmod{2^{10}}$ oluşur. Ancak hala şifreli metindir.

Gözlem anahtarı 2^9

Gözlem anaharı kullanıldığında oluşan mesaj

$133^{(14113671)^{2^9}} = 133^{2^{10}.(k.m+k+m)+1} \equiv x \pmod{2^{10}}$

Bu denklikten dolayı $\Phi(2^n) = 2^{n-1}$

M=133 çıkar. Oriiinal karakter kodu