Şimdiye kadar gördüğümüz sistemlere göre daha zor kırılabilen Vigenere kripto sistemini inceleyelim.

2.4. Vigenere Kripto Sistemi

Vigenere kripto sistemi adını 16.yy da yaşamış Blaise de Vigenere den almıştır. Şimdiye kadar görmüş olduğumuz kripto sistemlerde bir anahtar seçildikten sonra açık yazıdaki herbir harf kapalı yazıdaki tek bir harfe dönüştürülmüştür. Bu nedenle bu tip kripto sistemlere "**mono alfabetik**" kripto sistemler denir. Vigenere kripto sistemi mono alfabetik bir kripto sistem değildir.

Öncelikle açık yazı Çizelge 1.2.1'den kodlanır. Vigenere kripto sisteminde k anahtarı, m uzunlukta bir anahtar kelime olacak. Açık yazı, m uzunluğunda bloklara ayrıldıktan sonra her bir defada belirlenen anahtar kullanılarak m uzunluğundaki bu bloklar kapatılır. Dolayısıyla bir harf farklı farklı harflere dönüşebilir. Bu tip kripto sistemlere "**poli alfabetik**" kripto sistemler denir. Genel olarak, poli alfabetik sistem için kripto analiz mono alfabetik sistem için kripto analizden daha zordur.

Vigenere kripto sistemin özeti

$m \in \mathbb{Z}^+$ olsun. $\mathcal{P} = \mathcal{C} = \mathcal{K} =(\mathbb{Z}_{26})^m$ olmak üzere

$k = (k_1, k_2, ..., k_m) \in \mathcal{K}$ için kapama ve açma fonksiyonları sırasıyla

$$e_k(x_1, x_2, .., x_m) := (x_1 + k_1, x_2 + k_2, ..., x_m + k_{m)}$$

ve

$$d_k(y_1, y_2, .., y_m) := (y_1 - k_1, y_2 - k_2, ..., y_m - k_{m)}$$

olarak tanımlanırlar. Buradaki işlemler mod 26 'ya göre yapılır.

Örnek 2.4.1.

m=6 ve anahtar-kelime CIPHER olsun. Anahtar kelimeyi kodlarsak $k = (2, 8, 15, 7, 14, 17)$ olur. Açık yazı "thiscryptosystemisnotsecure" olsun. Şimdi açık yazıyı kapatalım. Öncelikle açık yazıyı kodlayıp $m = 6$ lı bloklara ayırmalıyız.

19	7	8	18	2	17	|	24	15	19	14	18	24	(Açık yazı)
2	8	15	7	14	17	|	2	8	15	7	14	17	(Kapatma)
21	15	23	25	6	8	|	0	23	8	21	22	15	(Kapalı yazı)

18	19	4	12	8	18	|	13	14	19	18	4	2	(Açık yazı)
2	8	15	7	14	17	|	2	8	15	7	14	17	(Kapatma)
20	1	19	19	12	9	|	15	22	8	25	8	19	(Kapalı yazı)

20	17	4	(Açık yazı)
2	8	15	(Kapatma)
22	25	19	(Kapalı yazı)

Kapalı yazının harf karşılıklarını yazarsak kapalı yazıyı buluruz:

"VPXZGIAXIVWPUBTTMJPWIZITWZT".

Kapalı yazıyı açmak için aynı anahtar kelimeyi kullanacağız fakat bu sefer mod 26 da anahtar kelimesini kapalı yazıdan çıkararak açık yazıyı elde edeceğiz.

Burada m-uzunluktaki olası anahtarların sayısı 26^m dir. Örneğin m=5 için $|\mathcal{K}| > 10^7$ dir. Bu rakam oldukça büyüktür. Fakat bilgisayar kullanılarak bütün olası anahtarlar denenebilir. Şimdiye kadar gördüğümüz mono alfabetik kripto

sistemlerde açık yazıdaki bir harf, kapalı yazıda yalnızca bir harfe karşılık geliyordu. Vigenere kripto sistemde açık yazıdaki bir harf m tane alfabetik karakterden biriyle eşleşebilir. Örneğimize bakarsak, ilk t harfi ile V; ikinci t harfi ile I; üçüncü t harfi ile B; dördüncü t harfi ile I harfi eşleşmiştir.

2.5 Pohlig-Hellman Üstel (Exponentiation) Kripto Sistemi

Bu kripto sistem Pohlig ve Hellman tarafından 1976 yılında bulunmuştur. İngiliz alfabesindeki 26 harfi aşağıdaki gibi kodlayalım.

Çizelge 2.5.1. İngiliz alfabesinin iki basamaklı bir kodlaması

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
00	01	02	03	04	05	06	07	08	09	10	11	12
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

Şimdi Pohlig-Hellman üstel kripto sistemini tanımlayalım. p asal bir sayı olsun. M açık yazının sayısal karşılığını göstersin (Çizelge 2.5.1.'den her harf yerine iki basamaklı karşılığı alınır). M sayısının onluk tabandaki yazılışı

$$M = M_1 M_2 ... M_n$$

olsun. M sayısını $0 < m_i < p$ olacak şekilde

$$m_1 := M_1 M_2 ... M_i \ , \ m_2 := M_{i+1} M_{i+2} ... M_{2i}, ...$$

bloklarına ayıralım.

$k, \ 0 < k < p$ ve $ebob(k, p-1) = 1$ olacak şekilde bir tamsayı ve k^{-1}, $kk^{-1} \equiv 1 \pmod{p-1}$ kongrüansını sağlayan tamsayı olsun. k^{-1} Euclid bölme

algoritması (Bölüm 3) kullanılarak hesaplanabilir. m_i için kapama ve açma fonksiyonları sırasıyla

$$c_i := e_k(m_i) \equiv m_i^k \pmod p$$
$$d_{k^{-1}}(c_i) := (c_i)^{k^{-1}} \pmod p$$

olarak tanımlanır. Kapama ve açma fonksiyonları Mod p de üs alma algoritması olan

Algoritma 3.4 ile hızlı bir şekilde hesaplanabilir.

Şimdi açma ve kapama fonksiyonlarının $d_{k^{-1}}(e_k(m_i)) = m_i$ özelliğini sağladığını gösterelim :

$kk^{-1} \equiv 1 \pmod{p-1}$ olduğundan

(3.5.1.) $$kk^{-1} = t(p-1) + 1$$

olacak şekilde bir t tamsayısı vardır.

$$\begin{aligned} d_{k^{-1}}(e_k(m_i)) &\equiv d_{k^{-1}}(m_i^k) \pmod p \\ &\equiv (m_i^k)^{k^{-1}} \pmod p \end{aligned}$$

(3.5.1.) numaralı denklemi ve Euler teoremini (Bölüm 3) kullanırsak

$$\begin{aligned} d_{k^{-1}}(e_k(m_i)) &\equiv \left(m_i^{(p-1)}\right)^t m_i \pmod p \\ &\equiv m_i \pmod p \end{aligned}$$

dir.

Örnek 2.5.1.

$p = 4578971$ ve $k = 3317271$ olarak seçelim öyleki $ebob(4578971-1, 3317271) = 1$ dir. $k \cdot k^{-1} \equiv 1 \pmod{p-1}$ ifadesinden bölme algoritması kullanarak $k^{-1} = 573651$ sayısı bulunabilir. Göndereceğimiz açık yazı "beginattack" olsun. Açık yazının sayısal karşılığı Çizelge 2.5.1'den:

$$M = 010406081300191900021020.$$

m_i yi mümkün olduğu kadar büyük seçerek, $0 < m_i < p$ olacak şekilde M açık yazısını m_i bloklara bölelim . p asal sayısı yedi basamaklı olduğundan M açık yazısını 6 basamaklı bloklara bölelim. Eğer son blok 3 karaktere sahip değilse, 3 karaktere tamamlamak için rastgale karakterler eklenir. Çünkü bütün blokların aynı uzunlukta olması daha uygundur. Bu örnekte "u" harfini ekledik.

$$\begin{array}{rcccccccc} M = & 010406 & | & 081300 & | & 191900 & | & 021020 \\ & m_1 & & m_2 & & m_3 & & m_4 \end{array}$$

$c_i = e_k(m_i) \equiv m_i^k \pmod{p}$ kapama fonksiyonunu her bir x_i için uygularsak kapalı yazıyı buluruz :

$$\begin{array}{rcccccccc} C = & 4137884 & | & 0438421 & | & 3227477 & | & 233970 \\ & c_1 & & c_2 & & c_3 & & c_4 \end{array}$$

olduğundan

$$C = 413788404384213227477233970 \text{ dir.}$$

Kapalı yazıyı önce $p = 7$ basamaklı bloklara böldükten sonra açma fonksiyonunu uygularsak açık yazıyı tekrar elde edebiliriz.