Çalışma Notları

Wednesday, November 6, 2019 7:04 PM

"Soldan sağa, sola sağa ilerler. ~ YEmreAk.com"

Tersinin Olması

- Aralarında asal denirler. (n⊥m)
- $\pi(x) = \frac{x}{\ln x}$

Modüler Aritmetik

- $a = r \pmod m$ → $a = qm + r$
- $\frac{a}{t} = \frac{b}{t} \pmod{\frac{m}{t}}$

$t = gcd(m, gcd(a,b))$

örnek

$14 = 8 \pmod 6$

$t = gcd(6, gcd(14,8)) = 2$

$9 = 4 \pmod 8$

Euclid Algoritması

$gcd(1180, 482) =$

$1180 = 2.482 + 216$

$482 = 2.216 + 50$

$216 = 4.50 + 16$

$50 = 3.16 + 2$

$16 = 8.2 + 0$ → 0'da dur

$gcd(\cdot) = 2$

Base of Algebra

$gcd(n,m) = s.n + t.m$ → $m^{-1} \pmod n$, $n^{-1} \pmod m$

$gcd(252, 198) = ?$ → 18

$252 = 1.198 + 54$

$198 = 3.54 + 36$

$54 = 1.36 + 18$

$36 = 2.18 + 0$ → $gcd(\cdot) = 18$

$18 = 54 - 1.36$

$18 = 54 - (198 - 3.54)$

$18 = 4(252 - 198) - 198$

$18 = 4.252 - 5.198$

$1 = 4.14 - 5.11$ → $14^{-1} \pmod{11}$, $11^{-1} \pmod{14}$

Extended Euclid Algoritması

$gcdext(87, 55) = \alpha$ ... $t = \ s =$

$(55, 32)$ → $87 \pmod{55}$

$(32, 23)$

$(23, 9)$

$(9, 5)$ $t_4 = 2$ $s_4 = -5$

$(5, 4)$

$(4, 1)$ $t = 0$ ← $s = t_0 - \lfloor n_1/m_1 \rfloor . s_0$

$(1, 0)$ $t = 1$ $s = 0$

$gcd(\cdot) = 1$

ilk gcdext'e kadar devam

$gcd(\cdot)$ $n^{-1} \pmod m$ $m^{-1} \pmod n$

$\alpha = t.n + m.s$

$t_n = s_{n-1}$

$s_n = t_{n-1} - \lfloor n_n / m_n \rfloor . s_{n-1}$ → büyük olan

→ Bu arada denklem atanırsa tersler bulunur.

23 ve 9 için

$1 = 23.2 + 19.(-5)$

$23^{-1} \pmod{19}$ $19^{-1} \pmod{23}$

Sözde Asallar

$2^{n-1} = 1 \pmod n$ → n asaldır.

→ Asallar uyar ama asal olmayanlar da uyabilir.

$2^{340} = 1 \pmod{341}$

$2^{10} = 1 \pmod{11}$ $2^{30} = 1 \pmod{31}$

$11 \perp 31$

$31.11 = 341$

Modüler Uzayda Kuvvet

- $x^2 = 1 \pmod{35}$

⇓

$x = \mp 1 \pmod 5$
$x = \mp 1 \pmod 7$ } Tüm asal çarpanları için yapılır. "$\Phi(m)$"

Chinese Remaining Theorem

$x = n_1 \pmod{m_1}$
$x = n_2 \pmod{m_2}$
⋮
$x = n_n \pmod{m_n}$

$M = \prod_{i=1}^{n} m_i$

$x = \sum_{i=0}^{n} n_i . \frac{M}{m_i} \left(\frac{M}{m_i}\right)^{-1} \pmod M$

sadeleştirme yapma ↑ ; m_i'ye göre tersi

Modüler Birim Elemanlar

Toplamada ∓ m → mod uzayı

Kuvvette ∓ $p-1$ → asal

$a = a + m$ $a^{-1} = a^{p-2}$

Fermat

p: asal ⇒ $a^{p-1} = 1 \pmod p$ ∧ $gcd(a,p) = 1$

Euler Fonksiyonu

→ 10'dan küçük 10 ile aralarında asal sayılar

$\Phi(10) = \{1, 3, 7, 9\}$

$\varphi(10) = 4$

$\varphi(p) = p - 1$

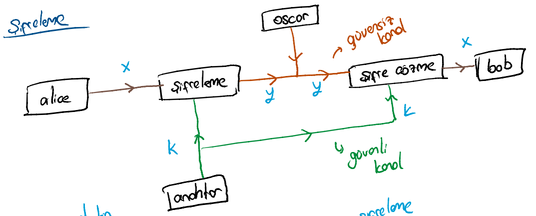
$\varphi(p^2) = p.(p-1)$

$\varphi(a.b) = \varphi(a).\varphi(b)$ → $a \perp b$

Euler-Fermat

$gcd(a,m) = 1$ ⇒ $a^{\varphi(m)} = 1 \pmod m$

Şifreleme



orijinal metin ← P: plain text

şifreli metin ← C: Cipher Text

K: Key Space → şifreleme anahtarı

E: Encryption → şifreleme

D: Decryption → şifre çözme

Shift Cipher

→ Kaydırmalı şifreleme → A→B, B→C

$y = e_k(x) = (x + k) \pmod m$

$x = e_k(y) = (y - k) \pmod m$

m: Anahtar uzayı

m'de kırılır

Substitution Cipher

→ Karıştırmalı şifreleme → A→X, B→C ⇒ X^{-1}→A, C^{-1}→B

$y = e_\pi(x) = \pi(x)$

$x = d_{\pi^{-1}}(x) = \pi^{-1}(x)$

m! 'de kırılır

Affine Cipher

→ Doğrusal denklemle şifreleme $(ax + b)$

→ $gcd(a,m) = 1$ olmalıdır.

$K: \{(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m \quad gcd(a,m) = 1\}$

$y = e_k(x) = (ax + b) \pmod m$

$x = d_k(y) = a^{-1}(y - b) \pmod m$

$\varphi(m).m$ de kırılır

örnek

$K = (7,3)$ $\mathbb{Z}_{26}$

$gcd(7,26) = 1$ olur.

$y = e_k(x) = 7x + 3 \pmod{26}$

$x = d_k(y) = 7^{-1}(y - 3) \pmod{26}$

7^{-1} ⇒ $gcdext(26, 7)$ $t = 3$ $s = -11$ → $7^{-1} \pmod{26}$

$(7,5)$ $t = -2$ $s = 3$

$(5,2)$ $t = 1$ $s = -2$

$(2,1)$ $t = 0$ $s = 1$

$(1,0)$ $t = 1$ $s = 0$

$x = d_k(y) = 15(y - 3) \pmod{26}$

$7.7 + 3 = 52 \pmod{26} = 0$

$e_k(\{HOT\}) = \{AXG\}$

$7 = 15(0 - 3) = -45 \pmod{26}$

Vigenere Cipher

→ Birden fazla toplama (batch sum)

$K = \{k_1, k_2, k_3 \dots k_n\}$ $P, C \subset (\mathbb{Z}_m)^n$

$e_k(x_1, x_2, x_3 \dots) = (x_1 + k_1, x_2 + k_2 \dots) \pmod m$

$d_k(y_1, y_2 \dots) = (y_1 - k_1, y_2 - k_2 \dots) \pmod m$

$(m)^n$ de kırılır

örnek

$K = \{2, 8, 15, 7, 4\}$

P =	t	h	i	s	...	
	19	7	8	2	...	
+	2	8	15	7	...	2 8 ...
	21	15	23	9	...	
C =	V	P	X	G	...	

Frekans Analizi

→ En sık kullanılan harfler belirlenir.

→ $X_{max} \to Y_{max}$ şeklinde x ve y değerleri konulur.

örnek

R→8
D→7
E,R,E→5
F,S,V = 4 } deşifre geçsin

C = "FMX..." 57 karakter

① R için

$e_k(x) = 17 \pmod{26}$

$e_k(x) = (ax + b) \pmod{26}$

$e_k(x) = (4a + b) \pmod{26}$

$4a + b = 17$

② D için

$e_k(x) = 3 \pmod{26}$

$e_k(x) = (19a + b) \pmod{26}$

$19a + b = 3$

Tahmin

$4a + b = 17$

$19a + b = 3$

$15a = 12 \pmod{26}$

$a = 6$ $b = 19$

→ $gcd(6, 26) \neq 1$ olduğundan seçim doğru değildir.

→ Cevap $a = 3$ $b = 5$ olduğundan ① onda doğrudur. (② yanlış)

Hill Cipher

Permutation Cipher

A→E, B→P E^{-1}→A, P^{-1}→B

(m) de ...

21 15 23 ...

C: V P X G ....

Hill Cipher

- Matrix ile şifreleme
- Det(K) ≠ 0 ve det(K) ⊥ m olmalıdır.

> K = { n x n, Z_m üzerinde tersi olan matrix }
>
> $y = e_K(x) = x \cdot K$ $\quad P, C \subset (Z_m)^n$
>
> $x = d_K(y) = y \cdot K^{-1}$

Matrix

$K^{-1} = \det(K) \cdot K^{T}$ $\qquad K = \det(K)^{-1} \cdot K^{-T}$

$\det(K) = \sum_{j=1}^{m} (-1)^{i+j} \cdot k_{ij} \cdot \det K_{ij}$

$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow K^{T} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$ $\qquad K \cdot K^{-1} = I$

- $\begin{smallmatrix} + & - \\ - & + \end{smallmatrix}$ çarptıktan sonra transpoz

Permutation Cipher

$A \to E$, $B \to P$ $\qquad E^{-1} \to A$, $P^{-1} \to B$

- "Hill Cipher"ın özel halidir.
- det(K) = 1 'dir
- "n"lik bloklara ayrılır "Substitution Cipher" uygulanır.

> K = { 1, 2, 3 ... n } 'e bağlı olarak oluşan permütasyon (π)
>
> $y = e_K(x_1, x_2, x_3 \dots x_n) = (x_{\pi(1)}, x_{\pi(2)} \dots)$ $\quad P, C \in (Z_m)^n$
>
> $x = d_K(y_1, y_2 \dots y_n) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)} \dots)$

örnek

	1 2 3 4 5 6	1 2 3 4 5 6	....
P:	s h e s e l	l s s e a s	
	3 5 1 6 4 2	3 5 1 6 4 2	....

C: e e s l s h

$K = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$ (satırlar 1, 2, 3, 4, 5, 6; sütunlar 3 5 1 6 4 2) $\qquad \det(K) = 1$

Stream Cipher

- Tek K yerine değişken K kullanılır. = "keystream"

(P, C, K, L, E, D)

> $z = \prod_{i=0}^{n} z_n$ $\qquad z \in L$
>
> $y = \prod_{i=0}^{n} e_{z_i}(x_i)$

AutoKey Cipher

- Üretici ile K 1 önceki X'e bağlıdır
- Olası hata, zincirleme sorun oluşturur.

> $g = \begin{cases} z_1 = K \\ z_i = x_{i+1}, & i \geq 2 \end{cases}$
>
> $y = e_K(x) = (x + z) \pmod m$
>
> $x = d_K(x) = (y - z) \pmod m$

(m)^x 'de tanılır → "Emin değilim (?)"

örnek

K = 8 $\quad$ P: "rendezvous", C = ? $\quad Z_{26}$

P: r e n d e z v o u s

17 4 13 3 ....

\+ 8 17 4 13

25 21 17 16

C: Z V R ...

One-Time Pad

- Exor işlemi yapılır
- $P, C, K \subset (Z_2)^n$

> $y = e_K(x) = \sum_{1}^{n} x_i + K_i \pmod 2$
>
> $x = d_K(y) = \sum_{i=1}^{n} y_i + K_i \pmod 2$

Substitution-Permutation Network