CENG 114 BİLGİSAYAR BİLİMLERİ İÇİN AYRIK YAPILAR

Doç. Dr. Tufan TURACI
tturaci@pau.edu.tr

- Pamukkale Üniversitesi
- Mühendislik Fakültesi
- Bilgisayar Mühendisliği Bölümü

- Hafta 12

Ders İçeriği

- **Hafta 10-11 Kısa tekrar (**Öklit Algoritması, Diyafont Denklem Çözümleri, Doğrusal Denklikler ve Çözümleri, Çinli Kalan Teoremi**)**
- **Sayılar Teorisi ile İlgili Önemli Teoremler**

  (Wilson Teoremi – Fermat Teoremi –Euler Teoremi)
- **Sayılar Teorisinin Kriptolojiye Uygulaması**

Öklit Algoritması

Teorem: $a \in \mathbb{Z}^+$, b ve $q \in \mathbb{Z}^+$ olsun.

$b = q.a + r$, $0 \leq r < a$ şartını sağlayan tek şekilde q ve r tamsayıları vardır.

$$\boxed{\begin{array}{cccc} b & q & a & r \\ 36 = & 3 & .10 & +6 \end{array}}$$

Tanım: $a, b, c \in \mathbb{Z}^+$ olsun.

$c|a$ ve $c|b$ ise c'ye a ile b'nin ortak bölenı denir.

Ortak bölenlerin en büyüğü (OBEB) gcd(a,b) veya (a,b) ile gösterilir.

= Öklid Algoritması =

Farzedelim ki $a, b \in \mathbb{Z}^+$ olsun. Aşağıdaki işlemler ardışık şekilde devam etsin.

$$a = b \cdot q_0 + r_0 \quad , \quad 0 \leq r_0 < b$$

$r_i, q_i \in \mathbb{Z}^+ \cup \{0\}$ olmak zorunda

$$b = r_0 \cdot q_1 + r_1 \quad , \quad 0 \leq r_1 < r_0$$

$$r_0 = r_1 \cdot q_2 + r_2 \quad , \quad 0 \leq r_2 < r_1$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$r_k = r_{k+1} q_{k+2} + r_{k+2} \quad , \quad 0 \leq r_{k+2} < r_{k+1}$$

Eğer $r_{k+2} = 0$ ise $\boxed{\gcd(a,b) = r_{k+1}\text{'dir.}}$

$$\gcd(205, 99) = ?$$

$$\overset{a}{205} = \overset{b}{99} \cdot 2 + \boxed{7}$$

$$\overset{a}{99} = \overset{b}{7} \cdot 14 + 1$$

$$7 = 1 \cdot 7 + \underline{\underline{0}}$$

$$\gcd(205, 99) = \underline{1}$$

Öklid algoritmasını kullanarak
$\gcd(203, 91)$'i hesaplayınız.

$203 = 91 \cdot 2 + 21$, $0 \leq 21 < 91$

$91 = 21 \cdot 4 + 7$, $0 \leq 7 < 21$

$21 = 7 \cdot 3 + \boxed{0}$

$\gcd(a,b) = 7$

gcd(a,b)=> greatest common divisor (Ortak bölenlerin en büyüğü - OBEB)

lcm(a,b)=> least common multiple (Ortak katların en küçüğü - OKEK)

Teorem: a ve b iki pozitif tamsayı olmak üzere

$$gcd(a,b)*lcm(a,b) = a*b$$

NOT: Öklit algoritması ve yukarıdaki teorem yardımıyla iki sayının OKEK değeri de bulunabilir.

Diyafont Denklemler

Tanım: $a, b, d \in \mathbb{Z}^+$, x, y bilinmeyen ve $x, y \in \mathbb{Z}$ olmak üzere: $\boxed{d = ax + by}$ şeklindeki denklemlere diyafont denklem denir.

Teorem: $a, b \in \mathbb{Z}^+$ ve $d = \gcd(a, b)$ olmak üzere; d, a ile b'nin lineer kombinasyonu şeklinde yazılabilir.

yani $d = a.x + b.y$'dir.

Örn $a=240$, $b=936$ olsun. $\gcd(a,b)=ax+by$

denkleminii sağlayan x ve y tamsayılarını bulunuz

$936 = 240.3 + 216$

$240 = 216.1 + 24 \longrightarrow \gcd(240,936) = 24$

$216 = 24.9 + 0$

$24 = 240x + 936y$ 'yi sağlayan x ve y değerleri?

$$\begin{aligned} 24 &= 240 - 216 \cdot 1 \\ &= 240 - (936 - 240 \cdot 3) \\ &= 240 - 936 + 240 \cdot 3 \\ &= \underset{x}{\boxed{4}} \cdot 240 + \underset{y}{\boxed{(-1)}}\, 936 \end{aligned}$$

Örn

$8 = 64x + 202 \cdot y$ eşitliğini sağlayan x ve y değerlerini öklid algoritmasını kullanarak hesaplayınız.

$$202 = 64 \cdot 3 + 10$$
$$64 = 10 \cdot 6 + 4$$
$$10 = 4 \cdot 2 + 2$$
$$4 = 2 \cdot 2 + 0$$

$$2 = 64x + 202y$$

$\Rightarrow$

$$2 = 10 - 4 \cdot 2$$
$$= 10 - (64 - 10 \cdot 6) \cdot 2$$
$$= 10 - 64 \cdot 2 + 10 \cdot 12$$
$$= 13 \cdot 10 - 64 \cdot 2$$

$$= 13 \cdot (202 - 64 \cdot 3) - 64 \cdot 2$$

$$= 13 \cdot 202 - 39 \cdot 64 - 64 \cdot 2$$

#4

$$2 = 13 \cdot 202 - 41 \cdot 64$$

$$8 = 52 \cdot 202 - 164 \cdot 64$$

$$= \underbrace{52}_{y} \cdot 202 + \underbrace{(-164)}_{x} \cdot 64$$

$$\boxed{\begin{aligned} x &= -164 \\ y &= 52 \end{aligned}}$$

Çalışma Sorusu: d= a.x+b.y şeklinde diyafont denklemleri çözen bir program yazınız. (d=gcd(a,b), a ve b pozitif tamsayılardır.)

Modüler Aritmetik

Tanım / $m \in \mathbb{Z}^+$ olsun. Eğer m sayısı 2 tamsayının farkı $a-b$'yi bölüyorsa, modül b'ye göre a denktir b denir ve $a \equiv b \pmod{m}$ şeklinde gösterilir.

$$\underset{a}{64} \equiv \underset{b}{4} \pmod{\underset{m}{10}}$$

$$m \mid a-b \overset{?}{=} 10 \mid 64-4$$

$$10 \mid 60 \checkmark$$

Doğrusal Denklikler

Tanım: $ax \equiv b \pmod{m}$ denkliğinin çözümü x_1 ise $a x_1 \equiv b \pmod{m}$ yazılabilir. Gerçekten x_1 bir çözüm ve $x_1 \equiv x_2 \pmod{m}$ ise, x_2'de bir çözümdür.

Bu durumda x_1 ve x_2 aynı çözüm sayılır.

Bunu $x \equiv x_1 \pmod{m}$ şeklinde gösterip, $ax \equiv b \pmod{m}$ denkliğinin çözümü diye okuruz.

(ör) $27 \equiv x \pmod 5$ ise $x = ?$

$\overset{\shortparallel}{2}$

2'nin denklik sınıfı $= \overline{2}$

$\overline{2} = 2 + 5k$ yani $\overline{2} = \{ \ldots, -3, \boxed{2}, 7, 12, \ldots \}$

(ör) $10.x \equiv 1 \pmod{13}$ ise $x = ?$

$x=1$ için sağlamaz

$x=2$ " "

$x=3$ " "

$x = \overline{4}$

$\boxed{x = 4 + 13k}$

$x=4$ sağlar

$40 \equiv 1 \pmod{13}$

$x = 4$

17

30

43

$\vdots$

x= 5,6,7,8,9,10,11 ve 12 için de sağlanmaz!!!

(ör) $11.x \equiv 28 \pmod{943}$ ise x'in çık?

Çözümü birazdan yapılacaktır…

Teorem: $ax \equiv b \pmod{m}$ denkliğinin bir çözümü olması demek $ax - my = b$ diyofant denkleminin bir çözümü olması demektir.

Örn: $10x \equiv 14 \pmod{24}$ ise $x = ?$

Çözüm: $\underset{a}{10}x \equiv \underset{b}{14} \pmod{\underset{m}{24}}$ ise $x = ?$

$\boxed{10x - 24y = 14}$ denkleminin çözümü olmamız gerekir.

$\downarrow$ 7 $\quad$ 7

→ diyofant denklem.

$24 = 10.2 + 4$

$10 = 4.2 + \boxed{2}$

$4 = 2.2 + 0$

$2 = 10 - 4.2$

$2 = 10 - (24 - 10.2).2$

$2 = 10 - 2.24 + 4.10$

$\underset{\text{obeb}}{2} = 5.\underset{x}{\,}\underset{a}{10} - 2.\underset{y}{\,}\underset{m}{24}$

7 ile çarpalım → $\underset{b}{14} = \underset{x}{\boxed{35.}}\underset{a}{10} - 14.\underset{y}{24}$

→ bir çözüm.

Böylece;

$$35 \equiv 11 \pmod{24}$$

$$\Downarrow$$

$$x = \overline{11} = \boxed{11 + 24k}$$

$$x = 11$$
$$x = 35$$
$$x = 59$$
$$x = 83$$
$$\vdots$$

elde edilir.

Örnek: $\underbrace{11}_{a}x \equiv \underbrace{28}_{b} \pmod{\underbrace{1943}_{m}}$ ise $x=?$

11x-1943y=28 diyafont denkleminin çözümünün olması gerekir.

$$1943 = 11.176 + 7$$
$$11 = 7.1 + 4$$
$$7 = 4.1 + 3$$
$$4 = 3.1 + \boxed{1}$$
obeb
$$3 = 1.3 + 0$$

$$1 = 4 - 3.1$$
$$1 = 4 - (7-4)$$
$$= 4.2 - 7$$
$$= (11-7).2 - 7$$
$$= 2.11 - 2.7 - 7$$
$$= 2.11 - 3.7$$
$$= 2.11 - 3.(1943 - 11.176)$$
$$= 2.11 + 528.11 - 3.1943$$
$$1 = 530.11 - 3.1943$$

Her iki taraf 28 ile çarpılırsa:

$$28 = \underbrace{14840}_{x} \cdot 11 - 84 \cdot 1943$$

$x \Rightarrow$ herhangi bir çözüm

$$14840 \equiv 1239 \pmod{1943}$$

$x = 1239$ yeni $x = 1239 + 1943k$

$x = 1239$

$x = 3182$

$\vdots$

elde edilir.

Çinli Kalan Teoremi

doğrusal denklik sistemlerini çözmek için bu teorem kullanılır. yani

$$\left.\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \end{aligned}\right\} \text{ denklik sistemi}$$

$x = ?$

Teorem:

$m_1, m_2, \ldots, m_r$ ikişer ikişer aralarında asal pozitif tam sayılar olsun.

$(m_i, m_j) = 1$ ve $i \neq j$ olsun.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

denklik sistemi mod $m = (m_1 \cdot m_2 \cdots m_r)$'ye göre bir tek çözüme sahiptir.

Bu çözüm

$$X = \left(\frac{m}{m_1}\right) \cdot a_1 \cdot b_1 + \left(\frac{m}{m_2}\right) \cdot a_2 \cdot b_2 + \cdots + \left(\frac{m}{m_r}\right) \cdot a_r \, b_r \text{ 'dir.}$$

b_i'ler için:

$\left(\frac{m}{m_i}\right) \cdot b_i \equiv 1 \pmod{m_i}$ formülü kullanılır.

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 5 \pmod 7$ ise $x = ?$ ($x = 68$ bir çözümdür. Kontrol ediniz...)

$a_1 = 2$ $m_1 = 3$ $m = 3 \cdot 5 \cdot 7 = 105$

$a_2 = 3$ $m_2 = 5$

$a_3 = 5$ $m_3 = 7$

$$X = \left(\frac{105}{3}\right) \cdot 2 \cdot b_1 + \left(\frac{105}{5}\right) \cdot 3 \cdot b_2 + \left(\frac{105}{7}\right) \cdot 5 \cdot b_3$$

$$X = 70 \cdot b_1 + 63 \cdot b_2 + 75 \cdot b_3$$

b_1

$$\left(\frac{105}{3}\right)\cdot b_1 \equiv 1 \pmod 3$$

$$35 \cdot b_1 \equiv 1 \pmod 3$$

$$\Downarrow$$

$$\boxed{b_1 = 2}$$

b_2

$$\left(\frac{105}{5}\right)\cdot b_2 \equiv 1 \pmod 5$$

$$21 \cdot b_2 \equiv 1 \pmod 5$$

$$\Downarrow$$

$$b_2 = 1$$

b_3

$$\left(\frac{105}{7}\right)\cdot b_3 \equiv 1 \pmod 7$$

$$15 \cdot b_3 \equiv 1 \pmod 7$$

$$\Downarrow$$

$$b_3 = 1$$

Böylece;

$$X = 70\,b_1 + 63\,b_2 + 75\,b_3$$

$$b_1 = 2,\quad b_2 = 1,\quad b_3 = 1$$

$$= 140 + 63 + 75 = 278$$

$$X \Rightarrow 278 \equiv 68 \pmod{105}$$

$$\boxed{x = 68 + 105k}$$

$$x = 68,\ 173,\ 278,\ 383\ ;$$ **elde edilir.**

Sayılar Teorisi ile İlgili Önemli Teoremler

Wilson Teoremi

$(\Rightarrow)$ p asal ise; $(p-1)! \equiv -1 \pmod{p}$

$(\Leftarrow)$ Eğer $(p-1)!+1 \equiv 0 \pmod{p}$ ise p asaldır.

Örn. $p=17$ ise $\boxed{16! \equiv -1 \pmod{17}}$

(Örn) $p=13$ sayısının asal sayı olduğunu wilson teoremi ile gösteriniz.

$$12! \equiv -1 \pmod{13}$$

$$12\cdot\cancel{11}\cdot\cancel{10}\cdot\cancel{9}\cdot\cancel{8}\cdot\cancel{7}\cdot\cancel{6}\cdot\cancel{5}\cdot\cancel{4}\cdot\cancel{3}\cdot\cancel{2}$$

$$4\cdot 10 \equiv 1 \pmod{13}$$
$$2\cdot 7 \equiv 1 \pmod{13}$$
$$3\cdot 9 \equiv 1 \pmod{13}$$
$$5\cdot 8 \equiv 1 \pmod{13}$$
$$6\cdot 11 \equiv 1 \pmod{13}$$

$$11! \equiv 1 \pmod{13}$$

$$12\cdot 11! \equiv 12 \pmod{13}$$

$$\boxed{12! \equiv -1 \pmod{13}}$$

Old.dan $p=13$ asaldır.

Fermat Teoremi

$\to$ p, a'yı bölmez.

p bir asal sayı ve $p \nmid a$ olsun. $a^{p-1} \equiv 1 \pmod{p}$'dir.

Buradan $a^p \equiv a \pmod{p}$ elde edilir.

Örn: $a=3$ $\quad 5 \nmid 3$ ✓

$p=5 \Rightarrow$ asal

$3^{5-1} \equiv 1 \pmod{5}$ $\Rightarrow$ $3^4 \equiv 1 \pmod{5}$

(4) in)

$5^{16} \equiv x \pmod{17}$ ise x'in en küçük 2 tamsayı değerinin toplamı nedir?

Fermat teo.dan $5^{16} \equiv 1 \pmod{17}$

$\bar{1} = 1 + 17k = 1, 18, 35, \ldots$ $\}$ $1 + 18 = 19$

Euler ϕ Fonksiyonu ve Euler Teoremi

Tanım: $m>1$ olmak üzere, $\phi(m)$ gösterimi m'den küçük ve m ile aralarında asal sayıların sayısını verir.
$\phi(1)=1$ olarak tanımlanır. ϕ fonksiyonu genellikle Euler ϕ fonk. olarak ifade edilir.

$\Rightarrow$ Her $m>1$ değeri için $\phi(m) \leq m-1$ 'dir. Eğer m asal ise $\phi(m) = m-1$ 'dir.

1 i)

$\phi(4) = ?$

$1-4$ ✓
$\cancel{2-4}$
$3-4$ ✓

$\phi(4) = 2$

$\phi(6) =$

$1-6$ ✓
$\cancel{2-6}$
$\cancel{3-6}$
$\cancel{4-6}$
$5-6$ ✓

$\phi(6) = 2$

$\phi(7) = 6$

$1-7$ ✓
$2-7$ ✓
$3-7$ ✓
$4-7$ ✓
$5-7$ ✓
$6-7$ ✓

aralarında asaldır!!

Teorem: m ve n aralarında asal 2 sayı ise

$\phi(m.n) = \phi(m).\phi(n)$ 'dir.

$$\phi(6) = \phi(3.2) = \phi(3).\phi(2)$$

$$= 2 . 1 = 2$$

$$\phi(15) = ? \quad \phi(3.5) = \phi(3).\phi(5)$$

$$= 2 . 4 = 8$$

Teorem: p asal ise $\phi(p^k) = p^k - p^{k-1}$'dir.

$\phi(125) = ?$ $\quad \phi(5^3) = 5^3 - 5^2$

$= 125 - 25 = \underline{100}$

Teorem $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ ise

$\phi(m) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r})$'dir. $\phi(m)$ çarpımsal bir fonk. old. dan;

$$\phi(m) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r})\text{'dir.}$$

(-1)$^{\text{IN}}$ $\phi(200) = ?$

$\phi(200) = \phi(2^3 \cdot 5^2) = \phi(2^3) \cdot \phi(5^2)$

$= (2^3 - 2^2) \cdot (5^2 - 5^1)$

$= (8 - 4) \cdot (25 - 5)$

$= 4 \cdot 20 = 80$

$\phi(75) = \phi(3 \cdot 5^2) = \phi(3) \cdot \phi(5^2)$

$= 2 \cdot 5^2 - 5^1$

$= 2 \cdot (25 - 5) = 2 \cdot 20 = 40$

Euler Teoremi: $m \in \mathbb{Z}^+$ ve $(m,a)=1$ olsun.

$$a^{\phi(m)} \equiv 1 \pmod{m}\text{'dir.}$$

Örn

$m=10$

$a=3$

$(3,10)=1$

$\phi(10)=\phi(5).\phi(2)$

$4.1=4$

$$3^{\phi(10)} \equiv 1 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

Sayılar Teorisi Uygulama
(Şifreleme Uygulamaları)

- Bilginin değiştirilerek korunması ile uğraşan bilim kriptoloji olarak adlandırılır.

- Elektronik ortamda bilginin korunması, çalınmasının önlenmesi büyük önem taşır.

- Klasik şifreleme genellikle
  - yerine koyma
  - yer değiştirme

mantığı ile çalışır.

* Bu şifrelemeye örnek olarak Sezar Şifresi (The Caesar cipher) gösterilebilir.

Sezar Şifreleme

Belirlenen bir anahtar değerine göre harflerin yer değiştirmesine dayalı bir şifreleme yöntemidir.

Harfler öncelikle numaralandırılır.

A → 0

B → 1

C → 2 (ingilizce Alfabesindeki harfler)

D → 3

⋮

Z → 25

Bir harfi şifrelemek için bir f fonksiyonu:

$$f(p) = (p+k)(\mathrm{mod}\ 26)$$

p, bir harfi temsil eder.

k, kaç birim öteleceğini temsil eder.

Şifre çözmek için fonksiyon:

$$f^{-1}(p) = (p-k)(\mathrm{mod}\ 26)$$

şeklindedir.

Örnek: DENIZLI kelimesini Sezar şifreleme ile şifreleyelim.

$\boxed{k=3 \text{ alalım}}$

$D \to 3$

$E \to 4$

$N \to 13$

$I \to 8$

$Z \to 25$

$L \to 11$

Tüm dizi: 3, 4, 13, 8, 25, 11, 8

Her sayıyı şifreleme:

$$f(p) = (p+k) \pmod{26}$$

$f(3)=6$, $f(4)=7$, $f(13)=16$, $f(8)=11$, $f(25)=2$, $f(11)=14$, olur.

Şifrelenmiş metin:

$6 \to G$, $7 \to H$, $16 \to Q$, $11 \to L$, $2 \to C$, $14 \to O$

Tüm dizi: 6, 7, 16, 11, 2, 14, 11

Şifrelenmiş metin: GHQLCOL şeklindedir.

Şifre Çözme:

GHQLCOL ve $k=3$.

sayılara çevir

6, 7, 16, 11, 2, 14, 11

Fonksiyon : $f^{-1}(p) = (p-k) \pmod{26}$

$f^{-1}(6) = 6-3 \pmod{26} = 3$

$f^{-1}(7) = 4$ $\qquad f^{-1}(11) = 8$ $\qquad f^{-1}(14) = 11$

$f^{-1}(16) = 13$ $\qquad f^{-1}(2) = 25$

Tüm dizi : 3, 4, 13, 8, 25, 11, 8

metin : DENIZLI

* Bu tip yöntemler kolaylıkla çözülebilir.

Güvenli bir kripto sistem genellikle Matematiksel açıdan çözümü zor olan NP problemlere dayalı olmalıdır.

RSA kriptosistemi büyük sayıları çarpanlara ayrılmasına dayalı bir yöntemdir.

RSA şifreleme

1977 yılında R. Rivest, A. Shamir ve L. Adleman tarafından geliştirilmiştir.

RSA algoritmasında anahtar üretimi aşağıdaki adımları içermelidir.

1) p ve q şeklinde iki tane büyük asal sayı seçiniz.
Büyük asal sayılar seçildiğinde
$p.q$'nun çarpanlara ayrılması zordur.

2) $n = p.q$ ve $\phi = (p-1).(q-1)$ hesaplanır.

3) $1 < e < \phi$ şeklinde $\gcd(e, \phi) = 1$ olacak şekilde rastgele bir e sayısı alınır.

4) $1 < d < \phi$ aralığında $e \cdot d \equiv 1 \pmod{\phi}$ şartını sağlayan d sayısı hesaplanır.

5) Böylece genel anahtar (n, e) özel anahtar d elde edilir.

Şifreleme:

1) Mesajın gönderileceği kişinin genel anahtarı (n,e) elde edilir.

2) Şifrelenecek mesaj $[0, n-1]$ aralığında bir m sayısına dönüştürülür.

3) $c = m^e \pmod{n}$ hesaplanır.

4) Oluşturulan c şifreli mesajı alıcıya gönderilir.

Deşifreleme:

1) d özel anahtarı ile $m = c^d (\bmod n)$ hesaplanır ve orjinal metin elde edilir.

RSA'nın güvenliği :

RSA sistemi n'nin çarpanlara ayrılması ile çözülebilir. Bu sayede gizli anahtar bulunabilir.

- n sayısı ne kadar büyükse sistem o kadar güvenlidir.
- $n = p \cdot q$ olduğundan çok büyük iki asal sayı alınırsa sistem güvenli olacaktır.

Örnek: Anahtar üretimi için

$p = 13$
$q = 23$ olsun.

$n = pq = 13 \cdot 23 = 299$ elde edilir.
$\phi = (p-1) \cdot (q-1) = 12 \cdot 22 = 264$ olur.

$gcd(e, \phi) = 1$ olacak şekilde $e = 35$ olsun.
$gcd(35, 299) = 1$ 'dir.

$35 \cdot d \equiv 1 \pmod{264}$ olacak şekilde

$d = 83$ elde ediyor.

$35 \cdot 83 = 2905$

$2905 \equiv 1 \pmod{264}$ şeklindedir.

Genel anahtar: $(299, 35)$

Özel anahtar: 83 elde edildi.

Zeka kelimesini RSA ile şifreleyelim.

ASCII kod tablosundan

z → 122

e → 101 $\Longrightarrow$ zeka kelimesi 122 101 107 057

k → 107 şeklinde yazılır.

a → 057

* Şifrelenecek sayılar n'den küçük olmalıdır.

Bu nedenle sayısal metin n'nin basamak sayısının bir eksik uzunluğundaki parçalara ayrılır.

- Bu sayı k'lar olarak adlandırılır.
- $n = 2537$ old. dan k'lar = 2 elde edilir.

Böylece: sayısal metin

12 21 01 10 70 97

şeklinde yazılır.

* Her blok k'lar basamaklı olmak zorundadır. Gerekirse sıfır eklenir.

Şifreleme:

$$12^{35} \equiv 259 \pmod{299}$$

$$21^{35} \equiv 226 \pmod{299}$$

$$01^{35} \equiv 1 \pmod{299}$$

$$10^{35} \equiv 119 \pmod{299}$$

$$70^{35} \equiv 47 \pmod{299}$$

$$97^{35} \equiv 297 \pmod{299}$$

yeni elde edilen değerler n ile aynı basamaklı olmalıdır. Bu sayı L_{cipher} olarak adlandırılır.

$L_{cipher} = 3$ elde edilir.

Böylece: 255 226 001 193 047 257 elde edilir.

Sonuç olarak

"Zeka" kelimesi için şifreli metin

255226001193047257

şeklindedir.

Deşifreleme:

Şifreli metin L_{cipher} uzunluklu bloklara ayrılır.

$$\boxed{259 \quad 226 \quad 001 \quad 199 \quad 047 \quad 297}$$

$m = c^d \pmod n$ uygulanır.

$$259^{83} \pmod{299} = 12$$

$$226^{83} \pmod{299} = 21$$

$$001^{83} \pmod{299} = 1$$

$$199^{83} \pmod{299} = 10$$

$$047^{83} \pmod{299} = 70$$

$$297^{83} \pmod{299} = 97$$

Bloklar 2 uzunlukta olmalıdır, gerekiyorsa sıfır eklenir.

12 21 01 10 70 97

⇓

12 21 01 10 70 97

⇓

122 101 107 097

" z e k a " elde edilir.

p ve q asal olmalıdır.

Asal olmaması durumunda algoritma çalışmaz.

Kaynaklar

- *Discrete Mathematics and Its Applications*, Kennet H. Rosen

(Ayrık Matematik ve Uygulamaları, Kennet H. Rosen (Türkçe çeviri), Palme yayıncılık)

- *Discrete Mathematics: Elementary and Beyond*, L. Lovász, J. Pelikán, K. Vesztergombi, 2003.

- *Introduction to Algorithms*, T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, 2009.

- *Introduction To Design And Analysis Of Algorithms*, A. Levitin, 2008.