Modular Arithmetic

i) $7 \bmod 4 = 3$

$-11 \bmod 7 = 7 - (11 \bmod 7)$

$= 7 - 4$

$= 3$

ii) Congruent Modulo.

Two integers a & b are said to be congruent modulo, if $(a \bmod n) \equiv (b \bmod n)$

$a \equiv (b \bmod n)$ or $b \equiv (a \bmod n)$

Properties of congruence

i) $a \equiv b \bmod n$ if n divides $(a-b)$

ii) $a \equiv b \bmod n$ implies $b \equiv a \bmod n$

iii) if $a \equiv b \bmod n$ and $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

Modular arithmetic operations/properties

i) $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

ii) $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

iii) $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Note → Exponentiated is performed by repeated multiplication

eg → $11^7 \bmod 13$

$\Rightarrow 11^2 = 121 \bmod 13 = 4$

$\Rightarrow (11^2)^2 = 11^4 \Rightarrow 4^2 \bmod 13 =$

$11^7 = (11^2 \times 11^2 \times 11^2 \times 11) \bmod 13$

$= ((121 \bmod 13) \times (121 \bmod 13) \times (121 \bmod 13) \times (11 \bmod 13)) \bmod 13$

$= (4 \times 4 \times 4 \times 4) \bmod 13$

$= (16 \bmod 13) \times (16 \bmod 13) \bmod 13$

$= (3 \times 3) \bmod 13$

$= 9$

iv) if $x \equiv y \bmod n$ & $a \equiv b \bmod n$, then,
$(x+a) \equiv (y+b) \bmod n$

v) if $x \equiv y \bmod n$ & $a = b \bmod n$, then,
$(x-a) \equiv (y-b) \bmod n$

Set of residues or residue classes modulo n

$Z_n = \{0, 1, 2, \ldots, (n-1)\}$

↓

each integer in Z_n represents a residue class

Euler's Totient function
(Euler's phi function) $\phi(n)$

→ defined as the no. of +ve integers less than n that are coprime to n $(n \geq 1)$

4 ← $\phi(5) = \{1, 2, 3, 4\}$ $\gcd\left(\begin{matrix}1\\2\\3\\4\end{matrix}\right\}, 5) = 1$.

2 ← $\phi(6) = \{1, 5\}$

↳ no. of elements in these sets is the totient function

★ coprime or mutually prime or relatively prime
$\gcd(a, b) = 1$.

→ when n → prime
$\phi(n) = n-1$

$\phi(23) = 23-1 = 22$

→ $\boxed{\phi(a*b) = \phi(a) * \phi(b)}$, but a & b should be coprime.

Euler's Theorem

→ also called Fermat-Euler theorem

→ Euler's Theorem states that if x and n are coprime positive integers, then

$\boxed{x^{\phi(n)} \equiv 1 \bmod n}$ → $x^{\phi(n)} \bmod n = 1 \bmod n$

where $\phi(n)$ = Euler's totient fn.

Eg→ $x = 11$, $n = 10$.

$11^{\phi(10)} \equiv 1 \bmod 10$

$11^4 \equiv 1 \bmod 10$

$14641 \equiv 1 \bmod 10$

which is true.

$\phi(10) = \phi(2) * \phi(5)$
$= 1 * 4$
$= 4$.

Note→ $\boxed{x^{\phi(n).a} \equiv 1 \bmod n}$ → multiple of $\phi(n)$ will give same result

Que- Solve $(4^{99} \bmod 35)$ by Euler Theorem.

$x^{\phi(n)} \equiv 1 \bmod n$ $\quad x=4, n=35$

$\Rightarrow 4^{\phi(35)} = 1 \bmod 35$ $\quad \phi(35) = \phi(7).\phi(5)$

$\Rightarrow 4^{24} = 1 \bmod 35$ — (1) $\quad = 6 \times 4$

$= 24$

$4^{99} \rightarrow 4^{24(4)} \cdot 4^3$

$4^{99} \bmod 35 = 4^{24\times4+3} \bmod 35$

$= ((4^{24})^4 \cdot 4^3) \bmod 35$

$= [(4^{24})^4 \bmod 35 \times 4^3 \bmod 35] \bmod 35$

(from eqn 1) $= [1 \bmod 35 \times 4^3 \bmod 35] \bmod 35$

$= (1 \times 4^3 \bmod 35) \bmod 35$

$= 64 \bmod 35$

$4^{99} \bmod 35 = (29) \bmod 35 = 29$ Ans

Ques- Solve $3^{302} \bmod 13$

$x = 3, \; n = 13$ $\qquad \phi(13) = 12$.

$x^{\phi(n)} \equiv 1 \bmod n$

$3^{12} = 1 \bmod 13$ — (1)

$\Rightarrow 3^{302} \bmod 13 = (3^{12\times16+10}) \bmod 13$

$= (3^{12})^{16} \cdot 3^{10} \bmod 13$

$= (3^{12})^{16} \bmod 13 \times 3^{10} \bmod 13$

$= 1 \bmod 13 \times (3^3 \times 3^3 \times 3^3 \times 3) \bmod 13$

$= 1 \times 3^3 \bmod 13 \times 3^3 \bmod 13 \times 3^3 \bmod 13 \times 3$

$= (1 \times 1 \times 1 \times 1 \times 3) \bmod 13.$

$= 3$ Ans

Fermat's Theorem

→ special case of euler's theorem.

→ If n is prime and x is a +ve integer not divisible by n, then

$$x^{n-1} \equiv 1 \bmod n$$ x, n are coprime

Another form of Fermat's Theorem,

$$x^n \equiv x \bmod n$$

Que- $x = 6$, $n = 7$

$$x^{n-1} \equiv 1 \bmod n$$

$$\Rightarrow 6^6 \equiv 1 \bmod 7$$

$6^6 \bmod 7 = 1 \bmod 7$ which is true

Que- $2^{16} \bmod 17$

$$x^{n-1} \equiv 1 \bmod n$$

$$2^{17-1} \equiv 1 \bmod 17$$

$$2^{16} \% 17 = 1 \bmod 17$$

$$2^{16} \% 17 = 1$$

Que- $2^{50} \bmod 17$

$$2^{16} \equiv 1 \bmod 17 \quad \text{— (1)}$$

$$2^{50} \bmod 17 = (2^{16})^3 \cdot 2^2 \bmod 17$$

$$= \left((2^{16})^3 \bmod 17 \times 2^2 \bmod 17\right) \bmod 17$$

$$= (1 \times 4) \bmod 17$$

$$= 4. \quad \text{Ans}$$

Rivest - Shamir - Adleman

RSA Algorithm

→ It is an asymmetric cryptographic algo (2 keys) i.e., public and private key concept
→ Public key → known to all users in network
Private key → kept secret not shareable to all.

★ If public key of user A is used for encryption, we have to use the private key of some user for decryption.

→ RSA scheme is block cipher.

Algorithm

1) Select two large prime nos. p and q
2) calculate $n = p * q$
3) calculate $\phi(n) = (p-1) * (q-1)$
4) choose value of e
   $1 < e < \phi(n)$ & $\gcd(\phi(n), e) = 1$
5) Calculate $d \equiv e^{-1} \bmod \phi(n) \rightarrow ed \equiv 1 \bmod \phi(n)$
6) public key = $\{e, n\}$
   private key = $\{d, n\}$

Encryption $C = M^e \bmod n$
Decryption $M = C^d \bmod n$

Cryptography

Symmetric Key / Secret Key

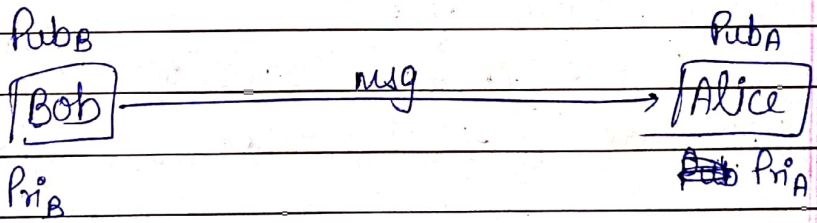
Asymmetric Key / Public Key

Asymmetric Key Cryptography

Six elements

→ Plain text
→ Encryption algo
→ Public key
→ Private key
→ Decryption algo

* Public key → to all users.
Private Key → known to particular user only



→ Encrypt msg with sender's public key & decrypt with receiver's private key.

eg → RSA & Diffie Hellman Key exchange algo

Advantages

1) key is not known to decrypt since diff. keys
2) key cannot be distributed
3) Easy to use for user

Disadvantages
→ use more resource
→ more mathematical calculation
→ slow compared to symmetric key

Application of Public Key Cryptography

1) Achieve Confidentiality (Encryption/ Decryption)
↳ only sender & receiver know the msg due to the use of different keys

2) Achieve Authentication (by digital signature)
↳ sender signs a message with his private key.

3) Key Exchange
↳ Sender & receiver exchange a session key, typically for conventional encryption.

Chinese Remainder Theorem

It states that there always exists an 'x' that satisfies the given congruence.

$x \equiv rem[0] \pmod{num[0]}$
$x \equiv rem[1] \pmod{num[1]}$
— — — —

& (num[0], num[1], ---, num[n-1]) all must be coprime to one another

eg→ $x \equiv 2 \mod 3$
$x \equiv 3 \mod 4$
$x \equiv 1 \mod 5$

↳ Check $\gcd(3,4) = \gcd(4,5) = \gcd(3,5) = 1$

So, here $x = 11$

Algorithm

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$

i) $\gcd(m_1, m_2) = \gcd(m_2, m_3) = \gcd(m_1, m_3) = 1$
all should be coprime

ii) $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_n x_n a_n) \bmod M$

$M = m_1 * m_2 * m_3 \cdots * m_n$

$M_i = \frac{M}{m_i}$ eg: $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$

To calculate x_i,
$M_i x_i \equiv 1 \mod m_i$ → Multiplicative inverse of M_i

Ques- $x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$
$x \equiv 3 \pmod{11}$

$\gcd(5,7) = \gcd(7,11) = \gcd(5,11) = 1$

$M = m_1 * m_2 * m_3 = 5 \times 7 \times 11 = 385$

$M_1 = \frac{M}{m_1} = \frac{5 \times 7 \times 11}{5} = 77$

$M_2 = \frac{5 \times 7 \times 11}{7} = 55$

$m_3 = \frac{5 \times 7 \times 11}{11} = 35$

$M_1 x_1 \equiv 1 \mod m_1$

$77 \times x_1 \equiv 1 \mod 5$

$\Rightarrow 77 x_1 \pmod 5 = 1$

$\Rightarrow [(77 \bmod 5) \times (x_1 \bmod 5)] \pmod 5 = 1$

$\Rightarrow 2 x_1 \pmod 5 = 1$

$x_1 = 3$

Similarly, $x_2 = 6$, $x_3 = 6$

Now, $x = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3) \bmod 385$

$= 1191 \bmod 385$

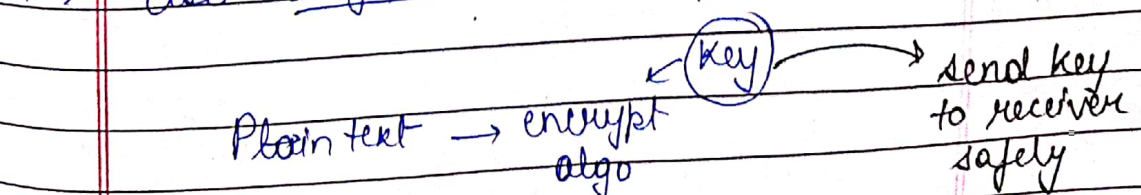
$x = 36$

Diffie-Hellman Key Exchange

→ not an encryption algo

→ used to exchange secret key b/w 2 users

→ use asymmetric encryption to exchange keys



Algorithm

1) Consider a prime number 'q'
2) Select 'α' such that it must be the primitive root of q & $\boxed{\alpha < q}$

★ let 'a' is a primitive root of q, then

$a^1 \bmod q$
$a^2 \bmod q$
$a^3 \bmod q$
⋮
$a^{q-1} \bmod q$

give results $\{1, 2, 3, \dots, q-1\}$ not particularly in order but all the values

$q = 7$

eg → $3^1 \bmod 7 = 3$ ✓
$3^2 \bmod 7 = 2$ ✓
$3^3 \bmod 7 = 6$ ✓
$3^4 \bmod 7 = 4$ ✓
$3^5 \bmod 7 = 5$ ✓
$3^6 \bmod 7 = 1$ ✓

Yes, 3 is a primitive root of 7

Values should not be repeated, all should be unique.

3) Now, α and q → global public elements (known to all)

X → private key
Y → Public key

5) Assume X_A (private key of A) and $X_A < q$
Calculate $\boxed{Y_A = \alpha^{X_A} \bmod q}$

6) Assume X_B (private key of B) and $X_B < q$
Calculate $\boxed{Y_B = \alpha^{X_B} \bmod q}$

Now we'll calculate secret keys which will be exchanged,
→ Calculate by the public keys.

$K_A = (Y_B)^{X_A} \bmod q$ — $K_B = (Y_A)^{X_B} \bmod q$

→ $K_A = K_B$ should be

Thus, the keys will be exchanged.

Cryptanalysis

Cryptanalysis is a technique of decoding messages from a non-readable format → readable format without knowing the key.

→ Recovering plain text without having access to the key.

There are various cryptanalytic attacks.

1) Cipher text only attack
Attacker only knows the cipher text

Differential cryptanalysis - type of chose plain text on block ciphers - analyze pairs of plain texts.

Integral cryptanalysis - sets of plain texts in which part of plain texts is kept constant but rest is modified (block ciphers)

ii) Known plain text only attack.
Attacker knows some combination of P_i, C_i & based on these, he tries to decrypt the messages.
(Linear Cryptanalysis)

iii) Chosen plain text attack. ~~(linear cryptanalysis)~~
Attacker: Randomly chooses plain texts to be encrypted and obtain the corresponding cipher texts.

iv) Chosen cipher text attack.
Attacker can analyze cipher text & gets their corresponding decryptions - plain texts

* The attacker has ability to make the victim decrypt any cipher text & send him back the result.

→ By these methods, attacker tries to guess the secret key.

Cryptology → study of codes, both creating & solving them.

Cryptography → encryption keys

Cryptanalysis → get plain text back without key

Side channel attack - depends on information collected from the physical system used to encrypt or decrypt

Dictionary attack - encrypting all the words from dictionary.

covered ← Steganos

writing ← graphia

Date
Page

Steganography

↳ information hide / covered writing

→ It is the practice of concealing messages, file, image (any type of information) within another file, message or image/ video.
Later, we will extract it at its destination

→ Use steganography and cryptography together can improve the security of the protected data/info & prevent detection of secret communication

Types
1) Text steganography
2) Audio "
3) Video "
4) Images "

How ?
→ Least Significant Bit