A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ascii 65

a-97 (1)

CNS

- Caesar cipher - Julius cipher
  - shifting letters in plaintext by certain no. of positions
  - known as shift / key
  - substitution cipher

- limited keyspace a-z, A-Z
- easy to crack

shift → 3

A → D

B → E

shift → 3

HELLO → PT

KHOOR → cipher

-3 -3 -3 -3 -3 ⟶ Decrypt

HELLO

eg: h e l l o

ch = h, offset = 'a' i.e 97

Int, ascii - h → 104

(ch - offset + shift) % 26 + offset

(104 - 97 + 3)

7 + 3

10 % 26

10 + offset

10 + 97

107 → i.e K (ascii)

h → K

2

- Playfair cipher - 1854
  - Charles Wheatstone
  - substitution cipher
  - encrypt pair of alphabets instead of single

- key: monarchy
- plaintext: instruments

1. Generate key square (5×5)
   - 5×5 grid of alphabets: acts as a key
   - each 25 alphabets must be unique
   - J is omitted, if J comes → I replaced

2. Algo to encrypt plaintext

if odd count, z is added at last

Plaintext: "instruments"

After split: 'in' 'st' 'ru' 'me' 'nt' 's z'

2 2 2 2 2

digraph

1. Pair with same letter x → not allowed

hello

he lx lo

add bogus letter

2. If letter is standing alone, add bogus letter

helloe

he lx lo ez

A B Max = 5

1

2

3

4

5

<u>Decrypt</u>

- shift back

encrypt (text, 26-shift)

(~~b~~, 23)
k

(ch - offset + shift) % 26 + offset

107 - 97 + 23

10 + 23

33 % 26 + 97

~~24 + 97 = 121~~

7 + 97 = 104 = i.e h

(ascii)

Solving:

in

	0	1	2	3	4
0	M	O	N	A	R
1	C	H	Y	B	D
2	E	F	G	I	K
3	L	P	Q	S	T
4	U	V	W	X	Z

digraph: 'in'

i → g

n → a

in → ga

st

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

if same row, next char

s → t

t → l

st → tl

ru → mz

me

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

if same col, next char bottom

m → c

e → l

me → cl

nt → rq

sz: tx

PT: instruments

CT: gatlmzclrqtx

Decrypt:

same row, char before

same col, char upper

else

take letters on horizontal opposite.

Decrypt:

turn ciphertext back into a vector

$\left[\quad \right]_{km} \times \left[\quad \right]_{ct_m} \% 26$

1. take inverse of key matrix
2. multiply it by cipher text matrix
3. reduce each ele. of resulting vector by mod 26

code:
1. processes 3 chunks of msg at a time
2. converts each char. to no.
3. multiply key matrix with message vector(3)
4. convert above resultant 3 chunk encrypted vector back to char and append to encrypted text.

A=0, B=1 . . . Z=25

(4)

Vigenere cipher - most designed to work with upper case char
- method of encrypting alphabetic text
- uses simple form of polyalphabetic substitution
* - encryption of original text is done using vignerere square or table

26 alphabets, 26 times ~~in dif~~, shifted cyclically each time

0	A - Z
1	B . . . Z A
2	C . . . Z A B
	D . . . Z A B C
.	
26	Z, A, B . . . Y

example: plaintext: GEEKSFORGEEKS n = 13
keyword: AYUSH

key: AYUSHAYUSHAYU n = 13
'AYUSH' repeated until length of the PT

GEE. . .
AYU. . .

i = G
j = A
→ search in table where row = G
col = A

A Y

G $\boxed{G}$ E $\boxed{C}$

G → G E → C

Programmatically ASCII val are considered

$\rightarrow (P_i + K_i) \% 26 +$ offset

i.e 'A' → 65

'a' → 97

E + y

$69 + 89 \% 26 + 65$

$\frac{158 \% 26}{2} + 65 \rightarrow 67 \rightarrow C$

Algebraically

Observe

(key)

(ci)

y

Plaintext (Row) E → C → cell

Encryption: ∴ $\boxed{(P_i + K_i) \% 26 = E_i}$

E → 4

y → 24

$(4 + 24) \% 26$

$28 \% 26$

$2 = E_i$

C → 2

∴ $E_i = C$

$C - y \quad \% 26$

Decryption: $D_i = \boxed{(E_i - K_i) \% 26}$

$= (2 - 24) \% 26$

$= -22 \% 26 = \underline{\underline{4}}$

4 → E

∴ E → original PT

③

Hill Cipher

- polygraphic substitution cipher (block cipher) based on linear algebra
- each letter replaced by a number %26 represented

$\boxed{A=0,\ B=1 \ldots Z=25}$

- process plaintext msg. in form of chunks
- ✲✲ - key matrix dimensions are chosen based on the chunk size of the PT you want to encrypt
- , len = n×n where n = plain text length

eg:

ACT

n=3

① key: GYBNQKURP

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

rowwise

② ACT is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

③ enciphered vector:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \begin{matrix} \%26 \\ \%26 \\ \%26 \end{matrix} \equiv \begin{bmatrix} 15 \\ 14 \\ \cancel{267} \end{bmatrix} \begin{matrix} \rightarrow P \\ \rightarrow O \\ \rightarrow H \end{matrix}$$

(5)

- Rail Fence

-zig-zag cipher i.e transposition cyphra

eg: rails=3 , PT: GEEKSFORGEEKS

no. of cols = len of plain text

1	G				S				G				S
2		E		K		F		R		E		K	
3			E				O				E		

ET: Rowise Read

GSGS EK FR EK EOE

Decryption:

* *

* * *

* *

colwise:

HELLOTHERE

rail vector of size 3 where 3==key

	0	1	2
rail:	H	E	L
	O	L	H
	R	T	
		E	
		E	

→ rows

e: HORELTEELH

Decryption:

pos(key,0)

r = ~~0~~ + ~~2~~ + ~~0~~ + ~~2~~ + ~~0~~ 1

d = ~~1~~ ~~-1~~ ~~1~~ ~~-1~~ 1

0 1 2 3 4 5 6 7 8 9
HOR ELTEE LH
n = 10

	0	1	2
pos:	0	0	0
1	1	1	1
	1	1	1
	1	1	
		1	
		1	

→ rows

→ Initially

3 5 2

~~0,1,2~~ i i

ind = 0

	0	1	2
rail:	H	E	L
	O	L	H
	R	T	
		E	
		E	

row i = 0

j = ~~0~~ + 2

ind = ~~0~~ + 2

row i = 1

j = ~~0~~ 1

Example:
primes: $p = 17$ $q = 11$

① $n = 187$ → find n

② Euler's totient
$\phi(n) = (p-1) * (q-1)$
$= (17-1) * (11-1)$
$= 16 * 10$
$= 160$

③ Choose val. of e
$1 < e < \phi n$ && $\gcd(\phi(n), e) = 1$

considering $e = 7$

$1 < 7 < \phi n$ $\gcd(\underbrace{160, 7}_{\text{co-prime}}) = 1$

④ Determine d
$d \equiv e^{-1} \bmod \phi n$
$de \equiv 1 \bmod \phi n$
$de \bmod \phi n = 1$
$(d * 7) \bmod 160 = 1$
$(23 * 7) \bmod 160 = 1$
$161 \bmod 160 = 1$ $\therefore \boxed{d = 23}$

MOD 3

RSA algorithm

- Rivest Shamir Adleman
- asymmetric cryptography

En:

Plaintext

$C = P^e \mod n$

ciphertext

IMP

* If en. is done using public key, the de. must be performed using private key of same user.

Algo:

1) Select 2 large prime nos p & q
2) cal. $n = p * q$
3. cal. $\phi(n) = (p-1) * (q-1)$ → euler's totient
4. choose value of e

$1 < e < \phi(n)$ and $\gcd(\underbrace{\phi(n), e}_{\text{co-prime}}) = 1$

≡ → congruent

5. calculate

$d \equiv e^{-1} \mod \phi(n)$ → Multiplicative inverse of d

i.e $ed \equiv 1 \mod \phi(n)$

→ $ed \mod \phi(n) = 1$

specific to user:

6. public key = $\{e, n\}$ → used in encryption

private key = $\{d, n\}$ → private key used for decryption

Encryption

$C = M^e \mod n$

public key of user A

Decryption

$M = C^d \mod n$

private key of user A

Numerical:

$c = 8$

$e = 13$

$n = 33$

$M = ?$

$M = c^d \bmod n$

→ 1. $n = 33$

$\therefore 11 \times 3 = 33$

$\therefore p = 3, \ q = 11$

2. <u>Euler's totient:</u>

$\phi(n) = (p-1) * (q-1)$

$= (3-1) * (11-1)$

$= 2 * 10$

$= 20$

3. determine d

d is mul.inv of $e \bmod \phi(n)$

$d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n)$

$de \bmod \phi(n) = 1$

$(d * \underset{13}{e}) \bmod 20 = 1$

$\therefore d = \underline{\underline{17}}$

$\therefore M = 8^{17} \bmod 33$

$\therefore M = 2$

- Diffie-Hellman key exchange algo.

- not an encryption algo
- symmetric key ~~exchange~~ encryption: requires secure & reliable channel for key exchange

shared

$$S^k \xrightarrow[\text{secure}]{k\ldots} R^k$$

symmetric

- public channel can be used to create a confidential shared key

- assy. en. is used to exchange the secret key

- Algorithm:

Initial param
1. consider a prime no. 'q'
2. select $\boxed{\alpha}$ such that it must be the primitive root of q and $\alpha < q$

'a' is a primitive root of q if

$a \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$ .... $a^{q-1} \bmod q$

gives results $\{1, 2, 3, \ldots, q-1\}$

if $q=7$, $a=3$

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

$\{3, 2, 6, 4, 1, 5\}$

$\therefore$ 3 is PR of 7

34 mod 26
ans — before decimal * 26

(3) ∴ public key = {e, n} → {7, 187}
private key {d, n} → {23, 187}

M = 88

M < N

Encryption:

$C = M^e \bmod n$
$= 88^7 \bmod 187$
$\underline{\underline{C = 11}}$

* see cal.

Decryption:
$M = C^d \bmod n$
$= 11^{23} \bmod 187$
$\underline{\underline{M = 88}}$

A: PK given, gen pub. key
B: PK given, gen pub. key

Example: 1

$\boxed{q = 7 \rightarrow prime}$

step 2. $\alpha < q$

$\alpha = 3$ or $\boxed{\alpha = 5}$

↑ is taken here

α & q are global, known to everyone

step (3.)

$x \rightarrow$ private key of user
$y \rightarrow$ public key of user

theory

assume x_A (private key) and $x_A < q$ of A (user)

calculate $\boxed{y_A = \alpha^{x_A} \mod q}$

App^n

key gen. of person)

Assume private key $\boxed{x_A = 3}$ $\because$ ($x_A < q$, $3 < 7$ yes)

$\therefore$ calculating public key $y_A = \alpha^{x_A} \mod q$

$= 5^3 \mod 7$

$\therefore \boxed{y_A = 6}$

step 4: assume $x_B \rightarrow$ PK of user B $x_B < q$

$\boxed{\text{Calculate public key} : y_B = \alpha^{x_B} \mod q}$

key generation of person 2

Let private key $\boxed{x_B = 4}$

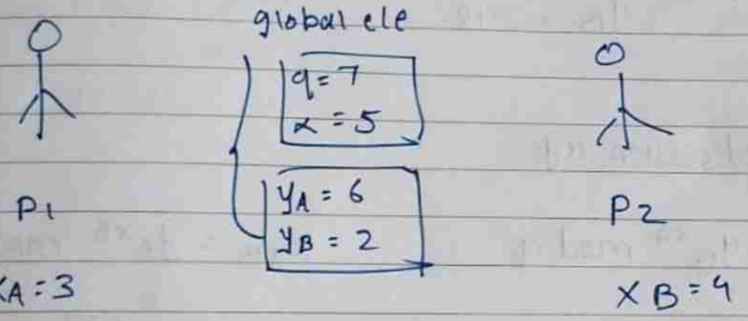
$(x_B < q)$
$(4 < 7)$

$\therefore$ Public key $\rightarrow y_B = \alpha^{x_B} \bmod q$

$= 5^4 \bmod 7$

$\therefore \boxed{y_B = 2}$

visualization:



(shared session key)

- 5. Now we'll calculate secret key
  - For this both sender & receiver uses public keys

person 1

$k_1 = (y_B)^{x_A} \bmod q$

user 2 pub. key

$= 2^3 \bmod 7$

$k_1 = 1$

person 2

$k_2 = (y_A)^{x_B} \bmod q$

user 1 public key

$= 6^4 \bmod 7$

$k_2 = 1$

As $k_1 == k_2$

Thus, keys are exchanged.

Eg: 2

$q = 353 \quad \alpha = 3$

$\therefore x_A = 97 \quad x_B = 233$

$\therefore$ Public key of A : $\alpha^{x_A} \bmod q$

$= 3^{97} \bmod 353$

$y_A = 40$

Public key of B : $\alpha^{x_B} \bmod q$

$= \cancel{23}\, 3^{233} \bmod 353$

$y_B = 248$

$\therefore$ Shared session key:

$K_{A} = y_B^{x_A} \bmod q$

$= 248^{97} \bmod 353$

$= \underline{160}$

$K_{AB} = y_A^{x_B} \bmod q$

$= 40^{233} \bmod 353$

$= \underline{160}$

283929

Eg: 3

$q = 17$

$\alpha = 5$

$x_A = 4$

$x_B = 6$

$7^1 \bmod 13 = 7$

$7^2 \bmod 13 = 10$

$7^3 \bmod 13 = 5$

$\vdots$

$7^{q-1} \bmod q$

$\therefore y_A = \alpha^{x_A} \bmod q$

$= 5^4 \bmod 17$

$y_A = 13$

$y_B = \alpha^{x_B} \bmod q$

$= 5^6 \bmod 17$

$y_B = 2$

$\therefore K_{AB} = {y_B}^{x_A} \bmod q$

$= 2^4 \bmod 17$

$= 16$

$K_{AB} = {y_A}^{x_B} \bmod q$

$= 13^6 \bmod 17$

$= 15.99\ldots\ldots$

≈ 16