Cryptography & Network Security.

31/07/19

K - matrix
K^{-1} - transpose of matrix.

$$k^{-1} = \frac{1}{|k|} \text{adj}(k^{-T}) \bmod 26$$

Extended Euclidean Algorithm (num, n).

Used to find multiplicative inverse of a given number.

* multiplicative inverse exist if and only if
GCD(num, n) = 1.

i=0 D=n R=num D-divisor R-remainder.

1) divide $\frac{D}{R}$ (is to be done until zero remainder is obtained).

Eg write in the format

Q(D) + R.

2) If i=0 then Pi (multiplicative inverse) = 0.

else if i=1 then Pi = 1

else $P_i = [P_{i-2} - P_{i-1}(Q_{i-2})] \bmod n$.

3) if R is not zero i++ and goto step 1.

4) $P_i = P_{i-2} - P_{i-1}(Q_{i-2}) \bmod n$.

Example.

i) $k = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ $k^{-1} = ?$

→ |k| = 15 - 6 = 9.

$$\text{adj}(k^T) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

Find multiplicative inverse of $|k|^{-1}$

$|k|^{-1} = ?$

$i=0 \quad \frac{26}{9} = 2(9)+8 \quad P_0 = 0$ $\quad$ num = 9, n = 26

$i=1 \quad \frac{9}{8} = 1(8)+1 \quad P_1 = 1$

$i=2 \quad \frac{8}{1} = 8(1)+0 \quad P_2 = P_{2-2} - P_{2-1}(Q_{i-2})$

$= 0 - 1(2) \bmod 26$

$= -2 \bmod 26$

$= 24.$

$P_3 = (1 - 24(1)) \bmod 26.$

$= -23 \bmod 26$

$= 3$

$$k^{-1} = 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 26$$

$$k^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

---

ii) $k = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ $\quad k^{-1} = ?$

$\rightarrow |k| = 63 - 20 = 43.$

$$\text{adj}(k^T) = \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}.$$

num = 43 n = 26.

$i = 0$ $\frac{26}{43} = 0(43) + 26$ $P_0 = 0$

$i = 1$ $\frac{43}{26} = 1(26) + 17$ $P_1 = 1$

$i = 2$ $\frac{26}{17} = 1(17) + 9$ $P_2 = 0 - 1(0) \mod 26$

$P_2 = 0$

$i = 3$ $\frac{17}{9} = 1(9) + 8$ $P_3 = 1 - 0(1) \mod 26$

$P_3 = 1$.

$i = 4$ $\frac{9}{8} = 1(8) + 1$ $P_4 = 0 - 1(1) \mod 26$

$P_4 = 25$.

$i = 5$ $\frac{8}{1} = 8(1) + 0$ $P_5 = 1 - 25(1) \mod 26$

$P_5 = 2$.

$P_6 = 25 - 2(1) \mod 26$

$= 23$.

$K^{-1} = 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \mod 26$

$K^{-1} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}_{3\times 3}$$

5×5

$$\begin{bmatrix} 1 & 2 & 3 & 1 & 2 \\ 4 & 5 & 6 & 4 & 5 \\ 7 & 8 & 9 & 7 & 8 \\ 1 & 2 & 3 & 1 & 2 \\ 4 & 5 & 6 & 4 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 5\times 9 - 8\times 6 & 8\times 3 - 2\times 9 & 2\times 6 - 3\times 5 \\ 6\times 7 - 9\times 4 & 9\times 1 - 7\times 3 & 3\times 4 - 6\times 1 \\ 4\times 8 - 7\times 5 & 7\times 2 - 8\times 1 & 1\times 5 - 4\times 9 \end{bmatrix}$$

$$\begin{bmatrix} 7 & 6 & 23 \\ 6 & 14 & 6 \\ 23 & 6 & 23 \end{bmatrix}$$

_____ × _____ × _____

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \\ 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{bmatrix}$$

$$\begin{bmatrix} 18\times19-21\times2 & 2\times5-19\times17 & 17\times21-5\times18 \\ 21\times2-21\times19 & 19\times17-2\times5 & 5\times21-17\times21 \\ 21\times2-18\times2 & 2\times17-2\times17 & 17\times18-21\times17 \end{bmatrix}$$

$$\text{Adj}(k) = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}.$$

$$|k| = 23$$

$$|k|^{-1} = 17.$$

Security Violation

* Unauthorised person accessing the data.
* Viewing the messages & transfering to the receiver.
* Unauthorised person constructing his own message & transfering to receiver.
* Holding the messages sent by the sender for undefined period of time.

Cryptography

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources.

* Confidentiality – * preserving the authorised restriction on information access from unauthorised restrictions.

* Types.

- Data confidentiality :- it ensures that secure data is not accessable by unauthorized person.
- Privacy :- ensures for whom the data to be disclosed.

* Integrity – * These objective guard against improper distortion of information.

* Types

- Data integrity.
- System integrity.

Availability: ensures that sim must work properly & it must provide service to an authorised person and it should not deny service to authorised person.

must ensure timely & reliable access.

Security breach is accessed on 3 levels

i) low level impact
ii) Moderate level impact
iii) High level impact.

low level - limited adverse effect on organization information/operation.

causes
- loss of financial loss.
- Addition equipments required
- minor harm to individual.

Moderate level - Result in significan effect to organizational asset.

causes
- doesn't have much effect on human life.

High level : - Senior effect on organizational asset.

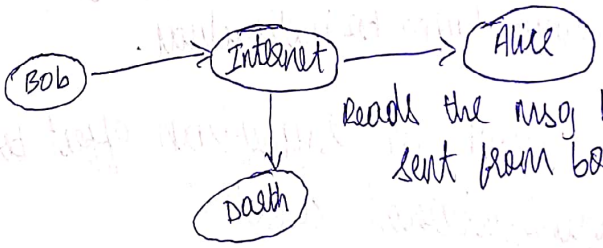
Challenges of Computer Security

- Requirements are difficult to understand & they are naturally complex.
- Exploiting weakness.
- Security agent must hold secret information.
- Protection of secret information.

OSI Security Architecture.

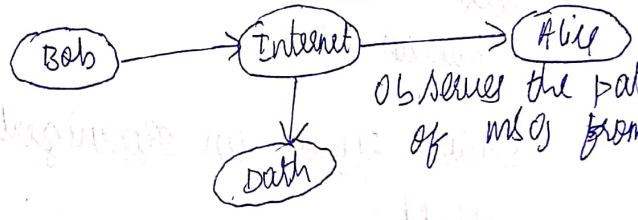
1) Security attacks.
   - Passive attack – Attempt to learn/make use of data (no disturbance to SYS)
     - Types:
       - Release message content
       - Traffic analysis.
   - Active attack – Attempt to alter system resources/ Effects operating of system.
2) Security services
3) Security mechanisms.

1)

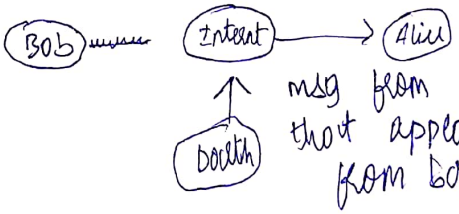


Reads the msg being sent from bob to alice.

2)



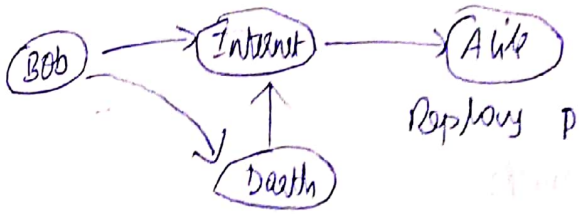
Observes the pattern of msgs from Bob to alice.



msg from Death that appears to be from Bob

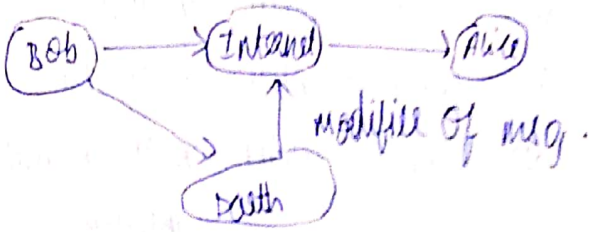
(Masquerade attack.)

4) Relay



Replays plays the msg Alice.

5) Modification of msg content.



6) Denial of service.

Security Services.

* Architecture follows X800 model.

i) Authentication Services.

- Sender - Receiver authentication.

There are two types of authentication service under X800

i) Peer entity authentication.
ii) Data origin authentication.

ii) Access control.

iii) Data confidentiality.

Types -

i) connection confidentiality.
ii) connection less confidentiality.
iii) Selective field confidentiality.

iv) Traffic flow confidentiality.

iv) Data Integrity.

5 Specific Services

i) connection integrity with recovery.
ii) connection integrity without recovery.
iii) selective field integrity.
iv) connectionless integrity
v) selective field connectionless integrity.

v) Non-Repudiation.

2specific services.

i) Non repudiation - origin.
ii) Non repudiation - destination.

Security mechanisms.

i) Encipherment

- Transforms on data from readable mode to non readable mode.

ii) Digital Signature

- Provides protection against duplication.

iii) Access control.

iv) Data integrity services.

v) Authentication exchange.

vi) Traffic padding.

vii) Routing control.

viii) Notarization.

ix) Trusted functionalities.

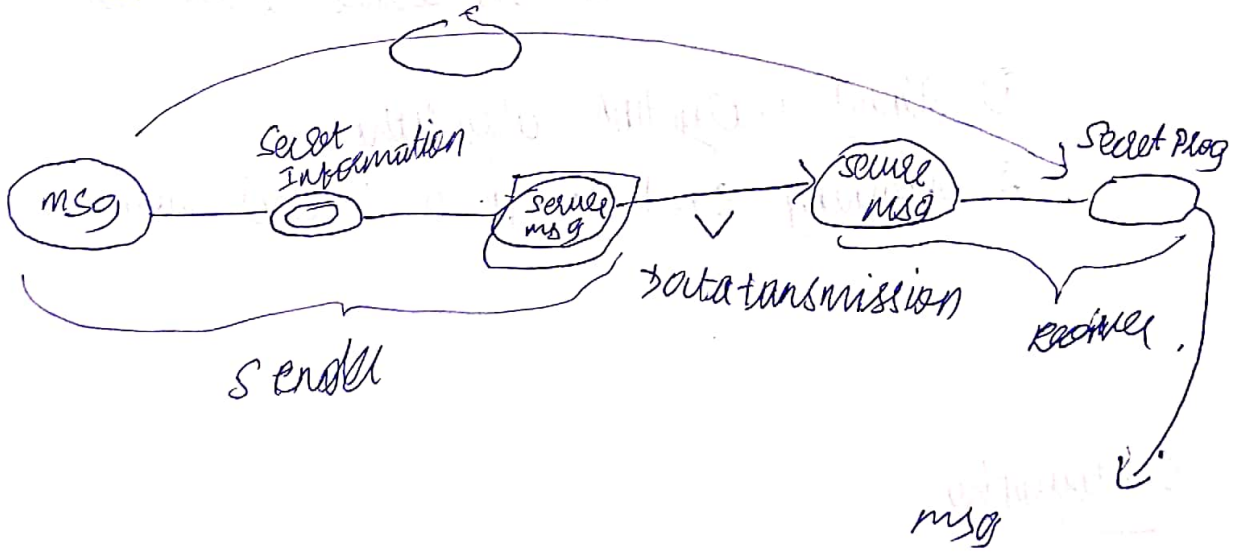
x) Event detection

xi) Security Audi trial.

xii) Security recovery.

OSI Security architecture.

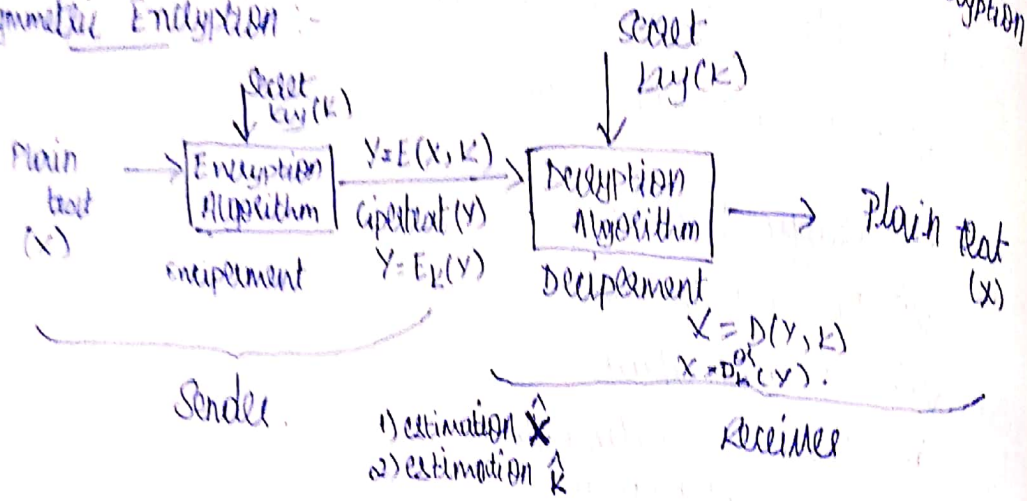
model for network security.



Classical Encryption Techniques

E - Encryption

Symmetric Encryption :-



Encipherment - process of converting plain text into ciphertext with the help of a secret key.

Decipherment - process of converting ciphertext into plain text with the help of a secret key.

* Sender & receiver must obtain the same secret key.

① Strong Encryption algorithm.
② Obtaining secret key in a secured fashion.

Cryptography

It is the study of different scheme used for encipherment process.

Characteristics :-

* type of operations.
  a) Substitution
  b) transposition.
* Product Systems : multiple stages of both substitution & transposition

② Number of keys used.

③ The way we use to process plaintext.

a) block process.

b) Stream Ciphes

Attacks on Cryptography.

There are two general aproches to attack cryptography

i) Cryptanalysis

- Based on nature of algorithm
- some knowledge about plain text, key & ciphes text.

ii) Brute force attack

- attacker will try every possible key on the ciphes text to obtain the plain text.

Symmetric Encryption Examples.

Substitution techniques.

i) caesar Ciphes.

$Y = (X + K) \bmod 26.$

$X = (Y - K) \bmod 26.$

Note:-
Only 25 possible key

ii) Monoalphabetic Ciphes.

X = textbook

S = {t, e, x, b, o, k}

Key Space = 6!

K = {0 k bt x}

③ Frequency Distribution

percentage of number of files in which it is obtained.

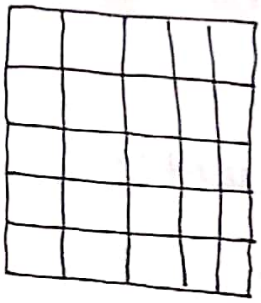
ciphertext ⇒ compute frequency

x => 12 5

t => 10 5

Playfair Cipher (for small msg)

- called as multiple letters encryption cipher.
- It process diagrams at a time.
- It is based on 5x5 matrix of letter constructed using keywords.



Eg:

keyword : monarchy

m	o	n	a	r
c	h	y	b	d
e	f	g	h	i/j
k	l	p	q	s
t				

m	o	n	a	r
c	h	y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

1. Repeating plaintext words

Ballon

Ba lx lo nx

Note:

* If repeating letters are there in a diagram, it must be replaced by 'x'.
* If it is ending with only one character then to make it a diagram 'x' is added.

2. Diagram fall in the same row
   ↳ replace letter to the right.

Eg: hb ⇒ yd.
ek ⇒ fc → matrix is wrapped rowwise

3. If diagram fall in same column
   ↳ replace the letter beneath.

Eg: hp ⇒ fv
ov ⇒ ho → matrix is wrapped column wise.
ix ⇒ sa

4. Otherwise → replace by elements of same row & the column is indicated by the other element.

Eg: fx ⇒ iv / jv

hj ⇒ bf

Example

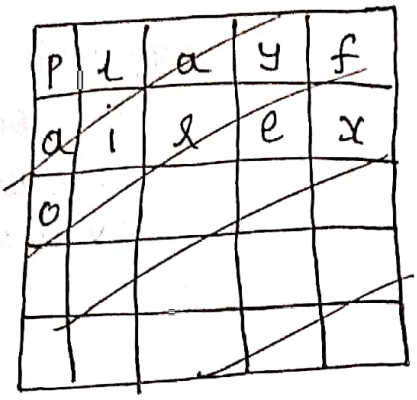
Ballon

Ba lx lo nx
ib su pm aw

Example 2

Key : playfair example

msg : Hide the gold



p	l	a	y	f
a	i	l	e	x
o				

p	l	a	y	f
i/j	l	e	x	m
b	c	d	g	h
k	n	o	q	s
t	u	v	w	z

Hi de th eg ol dx

bm od zb xd na ge

Cryptanalysis

* Attack rely on nature of algorithm.

Types

1. Ciphertext only attack
   - most difficult attack
   - the attacker knows only the ~~methanism for~~ algorithm & ciphertext.

2. known plaintext attack
   - the attacker knows the algorithm & some pair of plaintext ciphertext.

3. Choosen plaintext attack
   - the attacker insert his own msg to the system.

4. Choosen cipher text attack
   - insert cipher text & obtain corresponding plain text.

5. Choosen text
   - combination of 3 & 4.

Keysize

- Based on the effort required for brute force attack.

key size	Possible keys.	time required.
* 32 bits	$2^{32}-1$	35 mins
* 56 bits	$2^{56}-1$	1142 years.

Hill Cipher.

* multiletter cipher.

$C = P K \mod 26$

- K → key
- P → Plain text
- C → Cipher text.

$P = C K^{-1} \mod 26$

$K^{-1} = \det[K]^{-1} \; Adj[K^T]$

↳ multiplicative inverse of K

num = det[K]

EEA w.r.to 26

Step	i=0	26	D	Q(D)+R	P=0	P=1
		num	K			

$P_i = P_{i-2} - P_{i-1}(Q_{i-2}) \mod 26$

Example

Encrypt the msg = Hill Cipher using hill cipher technique with $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. Show calculation & result.

* Show calculation for the corresponding decryption of cipher text to recover the original pain text.

→ msg = Hill Cipher.

$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$C = \begin{bmatrix} 7 & 8 \\ 11 & 11 \\ 2 & 8 \\ 15 & 7 \\ 4 & 17 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \mod 26$

$$= \begin{bmatrix} 37 & 61 \\ 55 & 88 \\ 22 & 46 \\ 501 & 80 \\ 46 & 97 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 11 & 9 \\ 3 & 10 \\ 22 & 20 \\ 7 & 2 \\ 20 & 19 \end{bmatrix}$$

$= l\ j\ d\ k\ w\ e\ h\ c\ u\ t$

$K = \begin{bmatrix} d & d \\ c & f \end{bmatrix}$

$$K^{-1} = 9^{-1} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}.$$

$$P = C\ K^{-1} \bmod 26$$

$$P = \begin{bmatrix} 11 & 9 \\ 3 & 10 \\ 22 & 20 \\ 7 & 2 \\ 20 & 19 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 345 & 268 \\ 245 & 141 \\ 730 & 554 \\ 145 & 137 \\ 480 & 511 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \\ 2 & 8 \\ 15 & 7 \\ 4 & 17 \end{bmatrix} //$$

* Encrypt the msg = meet me now

$$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

* Show the calculations for the corresponding decryption of the cipher that to receive the original plain text

→ $$P = \begin{bmatrix} 12 & 4 \\ 4 & 19 \\ 12 & 4 \\ 13 & 14 \\ 22 & 23 \end{bmatrix} \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 128 & 76 \\ 131 & 149 \\ 128 & 76 \\ 187 & 150 \\ 313 & 249 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 24 & 24 \\ 1 & 19 \\ 24 & 24 \\ 5 & 20 \\ 1 & 15 \end{bmatrix} = yy\ bt\ yy\ fu\ bP$$

$$K^{-1} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$$

$$P = \begin{bmatrix} 24 & 24 \\ 1 & 19 \\ 24 & 24 \\ 5 & 20 \\ 1 & 15 \end{bmatrix} \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \text{ mod } 26$$

$$P = \begin{bmatrix} 480 & 888 \\ 290 & 487 \\ 480 & 888 \\ 325 & 560 \\ 230 & 387 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 12 & 4 \\ 4 & 19 \\ 12 & 4 \\ 13 & 14 \\ 22 & 23 \end{bmatrix}$$

Hill Ciphes.

msg : pay more money

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$C = \begin{bmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 303 & 303 & 521 \\ 532 & 490 & 677 \\ 348 & 312 & 538 \\ 353 & 341 & 605 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 17 & 7 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix} = rl\ lm\ wb\ kc\ sp\ dh$$

$P = CK^{-1} \bmod 26$ $\quad K^{-1} = \det[K]^{-1} \, Adj[K]$

$\det[K] = 23 - 9301 \bmod 26 = 23$

$\det[K]^{-1}$ = multiplicative inverse of 23 w.r.t 26

$i=0 \quad \frac{26}{23} = 1(23) + 3 \qquad P_0 = 0$

$i=1 \quad \frac{23}{3} = 7(3) + 2 \qquad P_1 = 1$

$i=2 \quad \frac{3}{2} = 1(2) + 1 \qquad P_2 = 0 - 1(1) \bmod 26 = 25.$

$i=3 \quad \frac{2}{1} = 2(1) + 0 \qquad P_3 = 1 - 25(7) \bmod 26 = 8.$

$P_4 = 17.$

$$K = \begin{bmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \\ 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{bmatrix}$$

$$\begin{bmatrix} 18\times19 - 21\times2 & 2\times5 - 19\times17 & 17\times21 - 5\times18 \\ 21\times2 - 21\times19 & 19\times17 - 2\times5 & 5\times21 - 17\times21 \\ 21\times2 - 18\times2 & 2\times17 - 2\times17 & 17\times18 - 21\times17 \end{bmatrix}$$

$$\begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \bmod 26$$

$$Adj(K) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}.$$

$$K^{-1} = 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}.$$

$$P = \begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \\ 15 & 3 & 7 \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 587 & 442 & 544 \\ 402 & 482 & 329 \\ 472 & 90 & 456 \\ 273 & 186 & 360 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 17 & 17 & 11 \\ 12 & 22 & 1 \\ 10 & 0 & 18 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{bmatrix}$$

= pay more money.

* msg = attack is tonight.

$$K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 01 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

C = PK mod 26.

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 551 & 247 & 646 \\ 130 & 38 & 204 \\ 555 & 318 & 789 \\ 374 & 289 & 637 \\ 329 & 199 & 562 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 5 & 13 & 22 \\ 0 & 12 & 22 \\ 0 & 6 & 9 \\ 0 & 3 & 13 \\ 10 & 17 & 16 \\ 17 & & \end{bmatrix}$$

= f n w a m w j g j k d ^ r r s

$\det(K) = -4287 \bmod 26 = -23 \bmod 26$

$= 3$.

$i = 0 \quad \frac{26}{3} = 8(3) + 2 \qquad P_0 = 0$

$P_1 = 1$

$i = 1 \quad \frac{3}{2} = 1(2) + 1$

$i = 2 \quad \frac{2}{1} = 2(1) + 0$

$P_2 = 0 - 1(8) \bmod 26$

$= 18$.

$P_3 = 1 - 18(8) \bmod 26$

$= -13 \bmod 26 = 13$