ADDITIVE CIPHER

Encryption $C = (P+K) \bmod 26$

Decryption $D = (C-K) \bmod 26$

eg:- Key ⇒ K = 3

Text ⇒ HELLO

P = 7 4 11 11 14

C = 10 7 14 14 17

K H O O R ⇒ Cipher Text

~~* Domain of key is 25~~

Now, decrypting it.

C = 10 7 14 14 17

D = 7 4 11 11 14

H E L L O

MULTIPLICATIVE CIPHER

Encryption $C = (P \times K) \bmod 26$

Decryption $D = (C \times K^{-1}) \bmod 26$

eg. Let key, K = 7

& Text, P = HELLO

P = 7 4 11 11 14

C = 23 2 25 25 20

X C Z Z U

Now, decryption –

C = 23 2 25 25 20

Multiplicative inverse of K :-

$t = t_1 - (q \times t_2)$

q	r_1	r_2	r	t_1	t_2	t
3	26	7	5	0	1	-3
1	7	5	2	1	-3	4
2	5	2	1	-3	4	-11
2	2	1	0	4	-11	26
	1	0		-11	26	

↑

-11 is the multiplicative inverse of 7.

but since it is negative add 26 to it

$K^{-1} = -11 + 26 = 15$

D = (23 × 15) mod 26	= 7	H
(2 × 15) mod 26	= 4	E
(25 × 15) mod 26	= 11	L
(25 × 15) mod 26	= 11	L
(20 × 15) mod 26	= 14	O

AFFINE CIPHER

- Rules :- ENCRYPTION
  $T = (P \times K_1) \bmod 26$
  $C = (T + K_2) \bmod 26$

  DECRYPTION
  $T = (C - K_2) \bmod 26$
  $P = (T \times K_1^{-1}) \bmod 26$

eg. Text ⇒ HELLO
7 4 11 11 14

$K_1 = 7$
$K_2 = 2$

$T = (7 \times 7) \bmod 26$ → 23 → X
$(4 \times 7) \bmod 26$ → 2 → C
$(11 \times 7) \bmod 26$ → 25 → Z
$(11 \times 7) \bmod 26$ → 25 → Z
$(14 \times 7) \bmod 26$ → 20 → U

C = 25 4 1 1 22
Z E B B W

Decryption :- T = 23 2 $\underbrace{-1 \bmod 26}_{(-1+26) \bmod 26 = 25}$ 25 20

finding K_1^{-1} $t = t_1 - (t_2 q)$

q	r_1	r_2	r	t_1	t_2	t
	26	7	5	0	1	-3
3	7	5	2	1	-3	4
1	5	2	1	-3	4	-11
2	2	1	0	4	-11	26
2	1	0		-11	26	

$K^{-1} = -11 + 26 = 15$

$P = (23 \times 15) \bmod 26$ → 7
$(2 \times 15) \bmod 26$ → 4
$(25 \times 15) \bmod 26$ → 11
$(25 \times 15) \bmod 26$ → 11
$(20 \times 15) \bmod 26$ → 14

7 4 11 11 14
H E L L O

HILL CIPHER

Key ⇒ MONA

M	O	N	A
C	H	Y	
E	F	P	
L			
U			

Text

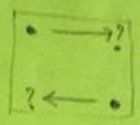
AIR CIPHER

Key ⇒ MONARCHY

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

* Two letters in same row -
  Replace by letters on immediate right
  Two letters in same column
  Replace by letters on immediate down

Else



Form a square & Replace dots by ?

Text ⇒ WE ARE DISCOVERED

write in pairs of 2.

WE AR ED IS CO VE RE DX

UG RM KC SX HM UF MK BZ

Cipher Text ⇒ UGRMKCSXHMUFMKBZ

To Decrypt - Follow same method

WE AR ED IS CO VE RE DX

WE ARE DISCOVERED

* If the keyword contains any repeating letter, omit that
  so PUZZLE would become PUZLE
  & SWIMMING SWIMNG

* If text contains repeating letters, separate them by X.

HILL CIPHER

Encryption - $C = (P \times K) \bmod 26$

Decryption :- $P = (C \times K^{-1}) \bmod 26$

"y" Message ⇒ ATTACK IS TONIGHT

Key ⇒ $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

P = 0 19 19 0 2 10 8 18 19 14 13 8 6 7 19

$$\begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}_{5\times3}$$

$$\begin{pmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{pmatrix}_{5\times3} \times \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}_{3\times3} = \begin{pmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{pmatrix} \Rightarrow \begin{matrix} F & N & W \\ A & G & W \\ J & G & J \\ K & D & N \\ R & R & Q \end{matrix}$$

Cipher Text = FNWAGWJGJ KDN RRQ

Decryption $\quad Key^{-1} = [Det(Key)]^{-1} \times Adj(Key)$

$$Det(Key) = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \bmod 26 = -1635 \bmod 26$$

$$= -23 \bmod 26$$

$$= 3$$

$key)]^{-1} = 3^{-1} \bmod 26$

$t = t_1 - (q t_2)$

q	r_1	r_2	r	t_1	t_2	t
8	26	3	2	0	1	-8
1	3	2	1	1	-8	9
2	2	1	0	-8	9	-26
	1	0		9	-26	

$3^{-1} = 9$

To find Adj (key) :-

$$\text{Transpose (key)} = \begin{bmatrix} 3 & 20 & 9 \\ 10 & 9 & 4 \\ 20 & 17 & 17 \end{bmatrix}$$

$$\text{Minor (key)} = \begin{bmatrix} 85 & 90 & -10 \\ 187 & -129 & -349 \\ -1 & -78 & -173 \end{bmatrix}$$

To find the Co-factor Matrix, put sign acc to $(-1)^{i+j}$

$$\text{Cofactor (key)} = \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} \Rightarrow \text{Adj(key)}$$

$$\text{Key}^{-1} = 9 \times \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 & 22 & 14 \\ 4 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}$$

$$\text{Text} = (C \times \text{Key}^{-1}) \bmod 26$$

$$\begin{bmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} \times \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 & 19 & \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

$$P \Rightarrow \begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix}$$

KEYED TRANSPOSITION CIPHER

MESSAGE : BUY SOME MILK AND EGGS

KEY ⇒ MONEY

{ so rows will have 5 chars since MONEY has 5 chars
& the order in which we will read characters will
be 2 4 3 1 5 since that's the order in which letters
of the key appear alphabetically }.

B U Y S O
M E M I L
K A N D E
G G S P K
Padding

To write the encrypted text, we see which column is to be written first & then so on.

S I D P B M K G Y M N S
U E A G O L E K

type the message: RHA VTN USR EDE AIE RIK
ATS ORR using the
keyword PRIZED

P R I Z E D
4 5 3 6 2 1

	4	5	3	6	2	1
R	A	I	R	S	T	R
	I	K	E	O	N	H
	E	A	D	Q	U	A
	R	T	F	R	S	V

[redacted]

Decrypted text - N E K R T D I Q

AIRSTRIKE ON HEADQUARTERS V

Keyless Transposition Cipher

Message: HELLO WORLD

H L O O L D
E L W R D

Cipher Text ⇒ H L O O L E L W R D

[redacted]

AES

128 bits → 10 rounds
192 bits → 12 "
256 bits → 14 "
} key size

Addroundkey
↓
4 steps
↓
3 steps without Mixcol.

for each round a state is given
convert PT to state — write all letters in hexadecimal — write col. wise

4 transformations :-

1) SubBytes

19	a0
3d	f4

S-Box is given so take value of each element & replace it by corresponding value from S-B

Eg. for 19 → row = 1 & col = 9
so if at that pos. val. is 36 then →

36	a0
32	f4

2) Shift Rows

$$\begin{bmatrix} 4 & 6 \\ 8 & 9 \end{bmatrix} \rightarrow \begin{bmatrix} 4 & 6 \\ 9 & 8 \end{bmatrix}$$

1st row → LS by 0
2nd row → LS by 1
3rd row → LS by 2

3) Mix Columns

$$(x^7 + x^6 + x^4 + x^2 + x)(x^5 + x^4 + x^2 + x)$$

(row → , col. ↓)

count mod 2 → odd – 1, even – 0

	1	2	4	5
1	2	3	5	6
2	3	4	6	7
4	5	6	8	9
6	7	8	10	11
7	8	9	11	12

1 0 1 0 1 0 1 0 1 0 0

Magic No. → $x^8 + x^4 + x^3 + x + 1$

= 1000 1011

```
   1 0 1 0 1 0 1 0 1 0 1 0 1 0 0
 ⊕ 1 0 0 0 1 1 0 1 1 1
   0 0 1 0 0 1 1 1 1 0 0 1 0 0
 ⊕ 1 0 0 0 1 1 0 1 1
     0 0 0 1 0 0 0 1 1 0 0
```

→ 1st col

$$\begin{bmatrix} 57 \\ 68 \\ 61 \\ 74 \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ - & - & - & \\ - & - & & \\ - & - & & \end{bmatrix} = \begin{bmatrix} (57.2) \oplus (68.3) \oplus (61.1) \oplus (74.1) \\ - \\ - \\ - \end{bmatrix}$$

(57.2)

$= (01010111).(10)$

$= (x^6+x^4+x^2+x+1).(x)$

0	1
1	2
2	3
4	5
6	7

10101110 < magic

$x^7+x^5+x^3+x^2+x$

Matrix State

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \times \begin{bmatrix} 9 & 9 & 9 \\ 9 & 9 & 9 \\ 0 & 1 & 0 \end{bmatrix}$$

$[1\ 2\ 3] \begin{bmatrix} 9 \\ 9 \\ 0 \end{bmatrix}$

$(1.9) \oplus (2.9) \oplus (3.0)$

(68.3)

$= (01101000).(11)$

4) Add Round

Above 4X4 ⊕ Round key (4X4) → New (4X4)

219324

Date 30/8/17
Page

Digital Signature

Zero Knowledge

~~Asymetric~~

Asymmetric

Public Key → encryption

Private Key → decryption

RSA

1) select 2 prime nos.

$p = 11$, $q = 5$

$n = p * q = 55$ → RSA modulus

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

Totient $= 40$

3) if e → public key let $e = 7$

then $1 < e < \phi(n)$ & $\gcd(e, \phi(n)) = 1$

4) if d → private key

$e * d \bmod \phi(n) = 1$

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

multiplicative inv. of e in domain $\phi(n)$

$$\frac{k(\phi(n)) + 1}{e}, \quad k = 1, 2, 3$$

when $k = 4 \Rightarrow \frac{4 \times 40 + 1}{7} = 23 = d$

Date 13/9/17
Page

$e \to 7$, $d \to 23$

PK $\to (e, n)$, PrK $\to (d, n)$

Message, $M = C^d \bmod n$ $\quad C \to$ cipher

$C = M^e \bmod n$

M → HIDE

7834

C → $7^7 \,\%\, 55 \to 28$

$8^7 \,\%\, 55 \to 2$

$3^7 \,\%\, 55 \to 42$

$4^7 \,\%\, 55 \to 49$

$(28^{23} \bmod n)$

$(28^{\downarrow 3} \times 28^5 \times 28^5 \times 28^5 \times 28^5) \bmod 55$

$(\downarrow 7 \times 43 \times 43 \times 43 \times 43) \,\%\, 55 \to 7$

Miller Rabin

Private key = p, q

Public = n

$c = p^2 \bmod n$

$p \bmod 4 = 3$

$q \bmod 4 = 3$

} $p, q \equiv 3 \bmod 4 = 3$ → don't proceed if doesn't satisfy

$\therefore p = 11$, $q = 7$

$n = p \times q = 77$

$C = p^2 \bmod n$

$= 45^2 \bmod 77 = 23$

Find a, b decryption

$a \times p + b \times q = 1$

3210

$f(x) =$

$g(x) =$

$h(\quad) =$

$m =$: 5

$P_0 =$

$h(P_0) = 3210$

1214 3210

$h^3(\quad) = 3210$

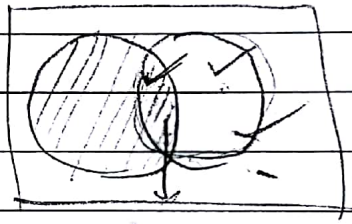
$h^3(P_0) =$ $h(3210) =$

$h^2(P_0) =$

3210

3200

$n = 1000$



gcd (11, 7)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	11	7	4	1	0	1	0		-1
1	7	4	3	0	1	-1	1	-1	2
1	4	3	1	1	-1	2	-1	2	-3
3	3	1	0	-1	2	-7	2	-3	11
	1	0		2	-7		-3	11	
				↓ a			↓ b		

$m_p = c^{(p+1)/4} \bmod p = 1$

$m_q = c^{(q+1)/4} \bmod q = 4$

$R_1 = (a \times m_q \times p + b \times m_p \times q) \bmod n = 67$

$R_2 = n - R_1 = 10$

$R_3 = (a \times m_q \times p - b \times m_p \times q) \bmod n = 32$

$R_4 = 45$

Apply hash fn. to all 4 to get 4 hash values.

If any hash value is equal to the hash value send by the sender then that is the plain text.

Q. $p = 23$, $q = 7$

$p = 24$

$23 \bmod 4 = 3$ ✓

$7 \bmod 4 = 3$ ✓

$n = p \times q = 161$

$C = 24^3 \bmod 161 = 93$

Decryption

gcd (23, 7)

q	r_1	r_2	r	t_1	t_2	t	s_1	s_2	s
3	23	7	2	0	1	-3	1	0	1
3	7	2	1	1	-3	10	0	1	-3
2	2	1	0	-3	10	-23	1	-3	7
	1	0		10	-23		-3	7	
				↓ b			↓ a		

$m_p = 93^{24/4} \bmod p = 1$

$m_q = 93^{8/4} \bmod q = 4$

$R_1 = (-3 \times 4 \times 23 + 10 \times 1 \times 7) \bmod 161 = 116$

$R_2 = 45$

$R_3 = 127$

$R_4 = 24$

Elgamal Cryptosystem

Alice → Bob

Public (e_1, e_2, p)

Private (d)

key generation

$p = 11$ {given}

$e_1 = 2 \in Z_p^*$ {given}

$d = 5 \in Z_p^*$ & $1 \le d \le p-2$

$Z_p^* = \{1, 2, 3, \ldots, 10\}$

compute e_2

$e_2 = e_1^d \bmod p$

$= 2^5 \bmod 11 = 10$

Public $(2, 10, 11)$

Encryption

$r = 4$, $m = 7$ {given}

$c_1 = e_1^r \bmod p$

$c_2 = (m \times e_2^r) \bmod p$

} 2 cipher texts are produced

$c_1 = 2^4 \bmod 11 = 5$

$c_2 = 7 \times 10^4 \bmod 11 = 7$

Decryption

$m = c_2 (c_1^d)^{-1} \bmod p$

$= c_2 c_1^{-d} \bmod p$

$= c_2 c_1^{p-1-d} \bmod p$ {$a^{-1} \bmod p = a^{p-2-1} \bmod p$}

$m = 7 \times 5^{11-1-5} \bmod 11 = 7$

Q. $p = 17$, $d = 5$, $e_1 = 6$, $m = 13$, $r = 10$ $6 \in Z_p^*$ ✓, $5 \in Z_p^*$ & $1 \le 5 \le 1$

$e_2 = 6^5 \bmod 17 = 7$

$c_1 = 6^{10} \bmod 17 = 15$

$c_2 = 13 \times 7^{10} \bmod 17 = 9$

$m = 9 \times 15^{17-1-5} \bmod 17$

$= 13$

Properties of Hash Function

1) Preimage Resistance – given a hash value h should not be able to get original image from hash value

2) Second Preimage Resistance – given a specific image M1 we should not be able to find another message M2 such that hash(M1) = hash(M2)

3) Collision Resistance – given any 2 msge. M1 & M2 we shouldn't find a relation such that hash(M1) = hash(M2)

Random Oracle Model

1) When a new msg. of any length is given to an oracle it creates a msg. digest randomly having 0's & 1's
2) When a msg. is given & digest exists, oracle simply gives the digest
3) No formula was used to create the digest

384
64K
1024

SHA – 512

→ the msg. should be less than 2^{128} bits otherwise this method fails
→ msg. should be in hexadecimal Eg → 'a' = 97 = 61
→ convert that into binary & calculate the length
→ write the length in hexadecimal

in hexa ↑ 128 bits ↑

[Msg] + [Padding] + [Length] } multiple of 1024

(Msg − 128) mod 1024 = Padding Bits

1 followed by 0's

~~16 X 64 bit~~
~~64 X 16~~ words is input → $w_0, w_1, \ldots, w_{15}$

1 word = 16 bits

64 bits words = 1024 bits

But 80 Rounds are there
16 words are to be expanded

Rot shift → circular right
→ shift ~~length~~ left ⇒ $W_{16} = W_{64}$

Rot Shift$_{1-8-7}(x)$ → Circular Right shift$_1$(x) ⊕ Circular Shift$_8$(x) ⊕ shift left$_7$(x)

bits

W_{i-16}, W_{i-15},

→ Take 1st 8 prime nos. & take square roots of them, convert the 16 decimal digits to hexa to get initial digest
→ Take 1st 80 prime nos. & take cube roots of them, convert the 16 decimal digits to hexa to get other digest

Classmate
Date 28/9/17
Page

→ Majority for creation of A & Conditional for creation of E

Majority

3 inputs of 4 bits is given

→ the 1st 3 bits (MSB → LSB) of all the 3 inputs are taken

→ if no. of 1's > 1 then majority bit is 1

→ if ——— <= 1 ——— 0

→ then the 4th bit (LSB) of all 3 inputs are taken & calculated the majority

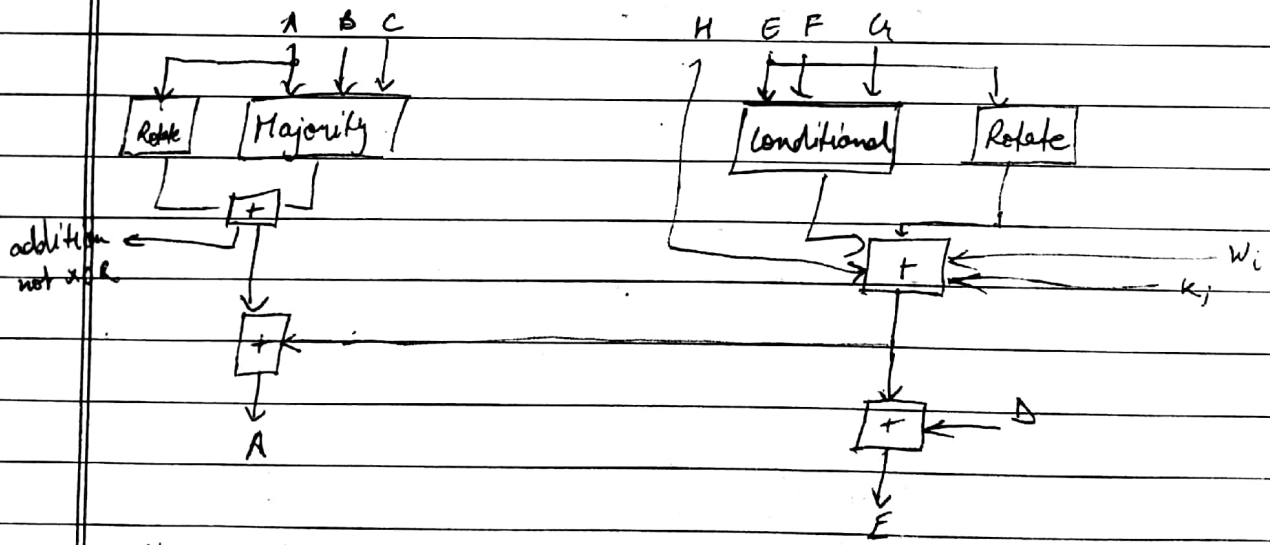
$$\text{Rotate}(A) = \text{Rotate}^{\text{Right}}_{28}(A) \oplus \text{Rotate}_{34}(A) \oplus \text{Rotate}_{39}(A)$$

E F G
1011 0100 1100

Conditional

if value of E = 1 → conditional val. = val. of F

if ——— = 0 → ——— = ——— G



After 79 th round the result generated is added to the initial digest.

Whirlpool

combination of AES & SHA

abcd

↓

4 - write this in 256 bits

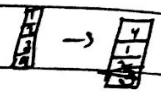
(- Msg - 256] mod 512 → length of padding

write msg. horizontally in matrix

Shift Column

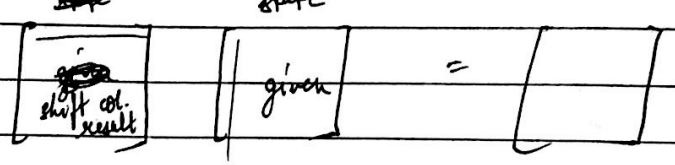
col 0 → no shift

col 1 → shift down by 1 bit



MixRows

state



Key Generation

RC = 8 X 8 matrix

$RC_{(0,j)} = SubBytes[8(round - 1) + col\ no.^{(j)}]$ $\quad 1 \le Round \le 10$

Digital Signature RSA

$d \rightarrow$ private

$e \rightarrow$ public

$S = M^d \bmod n$

$M = S^e \bmod n$

Q. $p = 7$, $q = 13$, $e = 5$, $M = 35$

$n = pq = 91$

$\phi(n) = (p-1)(q-1) = 72$

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

$$\frac{n \cdot \phi(n) + 1}{e} = 29 = d$$

Encryption

$S = M^d \bmod n$ (not public as in case of RSA)

$= 35^{29} \bmod 91$

Eg - $m^d \bmod n$

1) $d \rightarrow$ binary form

$29 \rightarrow 11101$

if 1st (MSB) dig. $= 1 \rightarrow$ calc. d^2, dm

if 1st dig. $= 0 \rightarrow$ calc. d^2

Round 1 $d_1 = 1$, $d = 1$ { initial val. of d is always 1 }

$\therefore d^2 = 1$ & $dm = 35$

Round 2 $d_2 = 1$, $d = 35$

$\therefore d^2 = 1225$ ~~& $dm = 1225$~~

if 1225 (d^2) $> n$

Then $d = 1225 \bmod n = 42$

$dm = 42 \times 35 = 1470 > n$

$\Rightarrow d = 1470 \bmod n = 14$

Round 3 $d_3 = 1$, $d = 14$

$\therefore d^2 = 196$

$\Rightarrow d = 196 \bmod n = 14$

$dm = 14 \times 35 \bmod n = 35$

Round 4 $d_4 = 0$, $d = 35$

$\therefore d^2 = 1225$

$\Rightarrow d = 42$

Round 5 $d_5 = 1$, $d = 42$

$d^0 = 42^2 \bmod n = 35$

$dm = 35^2$

$\Rightarrow d = 35^2 \bmod n$

$= 42$

$S = 42$

Decryption

$M = 42^5 \bmod 91$

Q. $p = 11$, $q = 13$, $e = 7$, $M = 9$

$d \rightarrow 103$

$S \rightarrow 113$

classmate
Date 13/10/17
Page

Elgamal DS

p, e_1, d, r

$e_2 = e_1^d \bmod p$

$s_1 = e_1^r \bmod p$

$s_2 = (M - ds_1)\, r^{-1} \bmod (p-1)$

$v_1 = e_1^M \bmod p$

$v_2 = e_2^{s_1} \times s_1^{s_2} \bmod p$

$v_1 \equiv v_2$

Q. $p = 19,\ e_1 = 10,\ d = 16,\ r = 5,\ M = 14$

$e_2 = 10^{16} \bmod 19 = 4$

$s_1 = 10^5 \bmod 19 = 3$

$s_2 = (14 - 16 \times 3)\, 5^{-1} \bmod 18$ (let do this)

$= (-34 \times 11) \bmod 18$

$= (11 \bmod 18)(-34 \bmod 18)$

$= 4$

$v_1 = 10^{14} \bmod 19 = 16$

$v_2 = 4^3 \times 3^4 \bmod 19 = 16$

{ $a.b \bmod x = a \bmod x \times b \bmod x$ }

Q. $M = 8,\ r = 5,\ p = 23,\ e_1 = 5,\ d = 3$

{ $e_2 = 10,\ s_1 = 10,\ s_2 = 16,\ v_1 \& v_2 = 16$ }

classmate
Date 20/10/17
Page

DS Schnorr

$p = 23$ {given}

$q = 11$, q is a factor of $p-1$ {given}

$(p-1) = 22$; 11 is a factor of 22

$e_1 = e_0^{(p-1)/q} \bmod p$ { if e_1 is not given & e_0 is given }

$e_1 = 2$ {given}

$d = 9$ {given}

$e_2 = e_1^d \bmod p = 6$

private → d

public → (e_1, e_2, p)

$r \rightarrow 3$, $M = 8$ {given}

$S_1 = h(M \mid e_1^r \bmod p)$

↓ concatenate

$e_1^r \bmod p = 8$

$\Rightarrow S_1 = h(88)$

$\Rightarrow S_1 = h(88) = 5$ {given}

$S_2 = (r + d \times S_1) \bmod q$

$= 4$

Decryption

$V \equiv S_1$

$V = h(M \mid e_1^{S_2} e_2^{-S_1} \bmod p)$

$= h(M \mid e_1^{S_2} e_2^{p-1-S_1} \bmod p)$

$= h(8 \mid 8)$