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

$f(x) =$

$g(x) =$

$h( ) =$

$m =$ : 5

$P_0 =$

$h(P_0) =$ 3210

1214 3210

$h^3(\ ) =$ "3210"

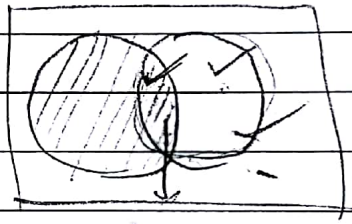
$h^3(P_0) =$ $h(3210) =$

$h^2(P_0) =$

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. $p = 17$, $d = 5$, $e_1 = 6$, $m = 13$, $r = 10$ $6 \in Z_p^*$ ✓, $5 \in Z_p^*$ & $1 \le 5 \le 16$

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

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

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

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

$= 13$

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

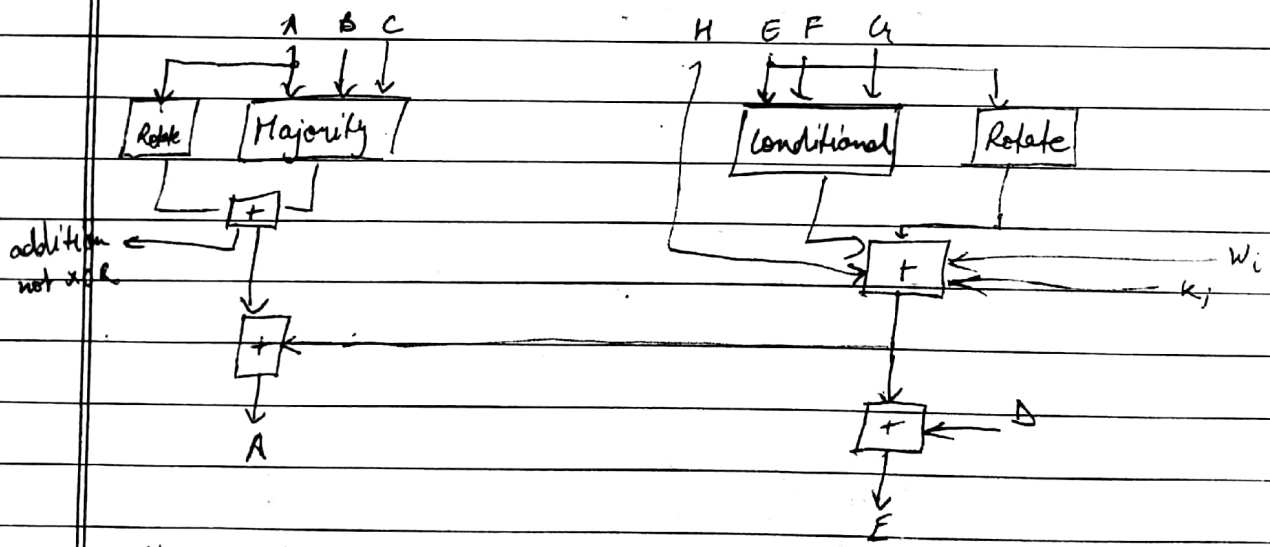
$$\text{Rotate}(A) = \text{Rotate}^{\text{Right}}_{28}(A) \oplus \text{Rotate}_{34}(A) \oplus \text{Rotate}_{39}(A)$$

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.