RSA

Step-1 Generate Public & Private Key

(i) Select 2 large prime numbers : p and q

(ii) modulus $n = p * q$

(iii) Euler's totient function : $\phi(n) = (p-1) * (q-1)$

(iv) Select e such that e is relatively prime to $\phi(n)$

$$1 < e < \phi(n)$$

(v) Determine d such that

$$d * e \equiv 1 (\mod[\phi(n)])$$

(vi) Public Key (PU) = $\{e, n\}$
Private Key (PR) = $\{d, n\}$

Eg-1 $p = 17$
$q = 19$

$n = 17 \times 19 = 323$
$\phi(n) = 16 \times 18 = 288$

$e = 7$

Public : $\{7, 323\}$
Private : $\{41, 323\}$

$7 \cdot d = 1 \mod(288)$

$$\boxed{d = 41}$$

Eg-2 $p = 29$
$q = 107$

$n = p * q = 29 \times 107$
$= (30-1)(100+7)$
$= 3000 + 37 - 107$
$= 3037 - 107$
$= 3030 - 100$
$n = 2930$

$\phi(n) = 28 \times 106$
$= (30-2)(100+6)$
$= 3000 + 180 - 200 - 12$
$= 3000 - 32$
$\phi(n) = 2968$

2967

$e = 3$

~~8~~ ~~3×e~~ $3 \times d = 1 \bmod (2968)$

$\boxed{d = 989}$
$\boxed{e = 3}$

Public : {3, 2930}
Private : {989, 2930}

2200 ~~2199~~

~~1003~~

Eg 3 $p = 157$
$q = 181$

$n = p \times q = 157 \times 181$

$n = 28,417$

$\phi(n) = 156 \times 180$
$= 28080$ 653

$e = 43$

$d * e \equiv 1 \bmod (28080)$

$\underset{d}{\underset{\downarrow}{653}} \times \underset{e}{\underset{\downarrow}{43}} = 1 \; [\bmod (28080)]$

$d = 653$

Public : (43, 28417)
Private ; (653, 28417)

Eg4 $p =$ ~~1009~~ 1009
$q =$ ~~1049~~ 1031

$n = 1009 \times 1031 = 1040279$

$\phi(n) = 1008 \times 1030 = 10,38,240$

$d = 167$
$e = 6217$

$167 \times 6217 \equiv 1 \mod (1040280)$

Step-2 Encrypt Message

$C = M^e \mod n$ → Public key

cipher text — Input Message

$M = 6$

eg $PU = \{e, n\} = \{7, 33\}$

$c = 6^7 \mod 33$
$= 279936 \mod 33$
$= 30$

Step-3 Decrypt Message

$\{d, n\}$

$M = C^d \mod n$ $PR = \{3, 33\}$

$= 30^3 \mod 33$

~~27000~~

$= 3^3 \mod 33$
$= 27 \mod 33$

$\boxed{M = 6}$

8 6 4 2 0 8 6 4 2 0 17 119 109

24 5

19 × 5

Eg : $p = 7$ $q = 19$ $M = 6$

(i) $n = 7 \times 19 = 133$

$\phi(n) = 6 \times 18 = 108$

$e = 17$ | $e = 5$

$\cancel{ed} = 1 \mod (108)$ | $5 \times 65 = 1 \mod 108$

89×17

$d = 89$ | $d = 65$

$PU = \{17, 123\}$
$PR = \{89, 133\}$

(ii) $C = M^e \mod n$
$= 6^{17} \mod 133$
$= \cancel{(6^3)^5 \, 6^2 \mod 133}$
$= \cancel{(83)^5 \cdot 36 \cdot \mod 133}$
$= \cancel{141}$

(ii) $C = M^e \mod n$
$= 6^5 \mod 133$
$= 7776 \mod 133$
$\boxed{C = 62}$

$p = 17 \quad q = 19 \qquad m = 15$

(iii) $P = c^d \bmod n$

$= 62^{65} \bmod 133$

$= 6$

$\Rightarrow (62)^2 = 3844$

$62^2 \bmod 133 = 120$

$\Rightarrow (62)^5 = 916132832 =$

RSA Example

$p = 7$
$q = 17$
$E = 5$
$M = 10$

$n = 7 \times 17 = 119$
$\phi(n) = 6 \times 16 = 96$

$e = 5$

$d \times e = 1 \pmod{n}$

$d \times 5 = 1 \bmod 96$

$\boxed{d = 77}$

3 (537)
4 (2151 2)
5 (860 504)
1600

$PU = \{5, 119\}$
$PR = \{77, 119\}$

$C = M^e \bmod n$

$= 10^5 \bmod 119$
$= 100000 \bmod 119$
$\boxed{C = 40}$

$P = C^d \bmod n$
$= 40^{77} \bmod 119$
$= \cancel{40^{25} \cdot 40^2 \bmod 119}$

~~53 mod 119~~

$40^5 \bmod 119 = 24$

Primitive Roots

$p = 7$ $\{0, 1, 2, 3, 4, 5, 6\}$

$3^1 = 3 \bmod 7 = 3$
$3^2 = 9 \bmod 7 = 2$
$3^3 = 27 \bmod 7 = 6$
$3^4 = 81 \bmod 7 = 4$
$3^5 = 243 \bmod 7 = 5$
$3^6 = 729 \bmod 7 = 1$

81
9
729

Diffie - Hellman Algorithm

(i) Take 2 large numbers [p & g are public]

p $\quad$ $g\ (2 <= g <= p-2)$

(ii) Users pick random private values x & y $(<p)$

(iii) Compute Public keys:

$$R_1 = g^x \bmod p$$
$$R_2 = g^y \bmod p$$

(iv) Keys R_1 & R_2 are exchanged

(v) Compute shared private key:

$$K_{alice} = (R_2)^x \bmod p$$
$$K_{bob} = (R_1)^y \bmod p$$

Algebraically $K_{alice} = K_{bob}$.

PROOF: $K_{alice} = K_{bob}$

$r_1 = g^x \bmod p$

$r_2 = g^y \bmod p$

$$K_1 = (g^y \bmod p)^x \bmod p$$
$$= g^{yx} \bmod p \bmod p$$
$$= g^{yx} \bmod p$$

$$K_2 = (g^x \bmod p)^y \bmod p$$
$$= g^{xy} \bmod p$$

128
5
640

Example : $p = 19 \quad g = 3$
$x = 15 \quad y = 10$

$R_1 = g^x \bmod p$ $\qquad R_1 = 12$
$R_2 = 16$

$= 3^{15} \bmod 19$
$= (3^3)^5 \bmod 19$

$\Rightarrow 3 \cdot (3^2 \bmod 19)^7 \bmod 19$
$\Rightarrow 3 \cdot (9 \bmod 19)^7 \bmod 19$

$\Rightarrow 3 \cdot (-10)^7 \bmod 19$
$\Rightarrow -3 (10)^7 \bmod 19$

$= \boxed{7}$

Q $p = 23 \quad g = 5$

$x = 15$
$y = 10$

$R_1 = g^x \bmod p$
$= 5^{15} \bmod 23$
$= 5 \cdot (5^2)^7 \bmod 23$
$= 5 (25 \bmod 23)^7 \bmod 23$
$= 5 \quad 2^7 \bmod 23$
$= 128 \times 5 \bmod 23$
$= 640 \bmod 23$
$\boxed{R_1 = 19}$

~~K alice~~ =

$R_2 = g^y \bmod p$

$= 5^{10} \bmod 23$

$= (5^2 \bmod 23)^5 \bmod 23$

$= 2^5 \bmod 23$

$\boxed{R_2 = 9}$

$K_{alice} = (R_2)^x \bmod p$

$= 9^{15} \bmod 23$

$= 9^3 \cdot (9^4 \bmod 23)^3 \bmod 23$

$= 9^3 \cdot 6^3 \bmod 23$

$= 9^3 \, (6^3 \bmod 23) \bmod 23$

$= 9^4 \bmod 23$

$\boxed{K_{alice} = 6}$

$K_{bob} = (R_1)^y \bmod p$

$= 19^{10} \bmod 23$

$= 19 \cdot (19^3 \bmod 23) \bmod 23$

$= 19 \cdot 5 \bmod 23$

$= 95 \bmod 23$

$\boxed{K_{bob} = 3}$

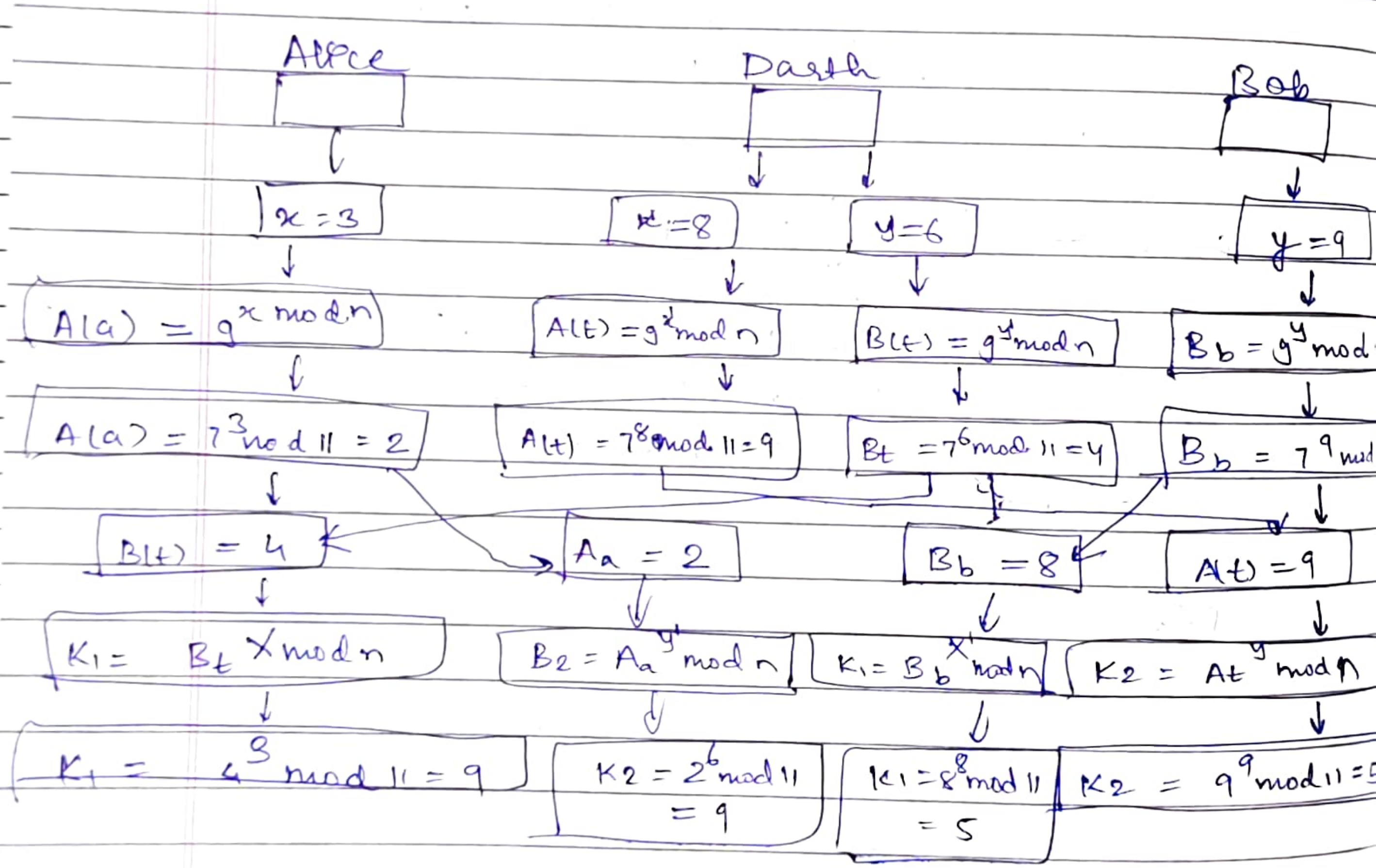
Now

Man in the Middle Attack

① Darth Prepares ~~XD1 & XD2~~ X_{D1} and X_{D2} and computes Y_{D1} and Y_{D2} (P|C)

② Alice transmits Y_a to Bob

③ Darth Intercepts Y_A & transmits Y_{D1}



ElGamal Encryption

☆ Keys & Parameters
- Domain parameter - $\{p, g\}$
- Choose $x \in [1, p-1]$ and compute $y = g^x \bmod p$
- Public key (p, g, y)
- Private key x

☆ Encryption $m \rightarrow (c_1, c_2)$
- Pick a random integer $k \in [1, p-1]$
- Compute $c_1 = g^k \bmod p$
- Compute $c_2 = m \times y^k \bmod p$

☆ Decryption
- $m = c_2 \times c_1^{-x} \bmod p$
- $c_2 \times c_1^{-x} = (m \times y^k) \times (g^k)^{-x}$
  $= m \times (g^x)^k \times (g^k)^{-x} = m \bmod p$

Q. $p = 23$
$g = 7$
$x = 9$

$y = g^x \bmod p$
$= 7^9 \bmod 23$
$= 7 \cdot (7^2)^4 \bmod 23$
$= 7 \cdot (49 \bmod 23)^4 \bmod 23$
$= 7 \cdot 3^4 \bmod 23$
$= 7 \cdot 3 \cdot (27 \bmod 23) \bmod 23$
$= 84 \bmod 23$
$\boxed{y = 15}$

$23 \overline{)84}$
69
15

Public Key : (23, 7, 15)

Private Key = 9

=> Encryption for m = 20

$K = 3$ (random)

$c_1 = 7^3 \bmod 23 = 21$

$= 7 \cdot 3 \bmod 23$

$= 21 \bmod 23$

$= 21$

$c_2 = 20 \times 15^3 \bmod 23$

$= 20 \times$

$c_2 = 18$

Send $(c_1, c_2) = (21, 18)$ as cipher text

=> Decryption

$M = 18 \times 21^{-9} \bmod 23$