Rabin Scheme(I)

- Select p, q = 3 mod 4
- n=pq, select b ($1 \le b \le n-1$)
- public ={n,b}, secret=p,q
- $e_k(x)$: x (x+b) mod n
- $d_k(y)$: $\sqrt{(b^2/4 + y)} - b/2 \bmod n$
- Choose one of 4 solutions
- Security = Factorization

Rabin Scheme(II)

(Ex) p=7, q=11, n=pq=77, b=9

$e_k(x)=x(x+9) \bmod 77$

$d_k(y)= \sqrt{(1+y)}-43 \bmod 77$

(Encryption) If y=22 $\rightarrow$ $\sqrt{23} \bmod 77$ $\rightarrow$ ± 10, $\pm$ 32 mod 77

(Decryption) Choose one of

10-43 mod 77=44, (77-10)-43 mod 77=24, 32-43 mod 77=66, (77-32)-43 mod 77=2 (not 1:1)

ElGamal Scheme(I)

- p : prime, $\alpha \in Z_p^*$: primitive element
  $\beta = \alpha^a \bmod p$
- p, α, β : public, a : secret
- select random int. $k \in Z_{p-1}$
- $e_K(x,k)=(y_1,y_2)$ where $y_1 = \alpha^k \bmod p$,
  $y_2 = x\beta^k \bmod p$
- $d_K(y_1,y_2)=y_2(y_1^a)^{-1} \bmod p$

ElGamal Scheme(II)

(Ex) $p=2579$, $\alpha=2$, $a=765$,
$\beta=2^{765} \bmod 2579 = 949$

(1) $x=1299$. Alice chooses $k=853$

(2) $y_1=2^{853} \bmod 2579=435$, $y_2=1299 \times 949^{853} \bmod 2579=2396$

(3) Bob receives (435,2396).
$x=2396 \times (435^{765})^{-1} \bmod 2579=1299$

Discrete Logarithm(I)

- **(Def)**

(Problem Instance) I=(p,α,β) where p is a prime, primitive element, $\alpha \in Z_p^*$ and $\beta \in Z_p^*$.

(Objective) Find the unique integer *a*, $0 \le a \le p-2$, such that

$$\alpha^{a} = \beta \bmod p.$$

We denote this integer, *a* by $\log_\alpha \beta$.

Discrete Logarithm(II)

- **Exhaustive Search : O(p) time, O(1) space**
- **Precomputed Table : O(1) time, O(p) space**
- **Time-memory Tradeoff by Shanks :**

O(1) time, O(p) pre-computation, O(p) memory

Shanks' algorithm for DLP(I)

Input : p, α, β,

Output : a where $\alpha^{a} = \beta$ mod p.

Let m = $\lceil \sqrt{(p-1)} \rceil$

1.compute α^{mj} mod p, $0 \le j \le m-1$

2.sort m ordered pairs (j, α^{mj} mod p) w.r.t. 2nd coordinates, obtaining list L_1

3.compute $\beta\alpha^{-i}$ mod p, $0 \le i \le m-1$

4.sort m ordered pairs (i, $\beta\alpha^{-i}$ mod p) w.r.t. 2nd coordinates, obtaining list L_2

5.find a pair (j,y) $\in L_1$ and a pair (i,y) $\in L_2$ (i.e., a pair having identical 2nd coordinates)

6.output mj +i mod(p-1).($\alpha^{mj} = y = \beta\alpha^{-i}$, $\alpha^{mj+i} = \beta \rightarrow \log_{\alpha}\beta = mj+i$)

*** Complexity : O(m) time, O(m) memory**

Shanks' algorithm for DLP(II)

(Ex.) p=809, find $\log_3 525$.

1. α=3, β=525, m = $\lceil \sqrt{(808)} \rceil$=29

2. α^{29} mod 809 = 99.

3. ordered pairs (j, 99^{j} mod 809) for $0 \le j \le 28$
(0,1), …,(10,644), ..,(28,81).

4. ordered pairs (i, 525 x$(3^{i})^{-1}$mod 809), $0 \le i \le 28$
(0,525), .., (19,644), ..,(28,163).

5. find match (10,644) in L_1 and (19,644) in L_2

6. thus, $\log_3 525$ = 29x10 + 19 =309

7. (Confirmation) 3^{309} = 525 mod 809

Other DLP Algorithm

- **Pohlig-Hellman Algorithm**
  - compute $p-1 = \prod_{i=1}^{k} p_i^{c_i}$
  - compute *a* mod $p_i^{c_i}$ $(1 \le i \le k)$
  - apply *a* mod (p-1) by CRT
- **Index-calculus Method**
  - find logarithms of primes in factor base
  - compute DL of desired element, using DL of elements in factor base.

Knapsack-based PKC

- **Weighted (or subset) Sum Problem**

(problem) $I=(s_1, \ldots, s_n, T)$ where s_i and T are integers, s_i :size T:target sum

(question) is there 0-1 vector $x=(x_1, \ldots x_n)$ s.t.,

$\prod_{i=1}^{n} x_i s_i = T$?

- **Scheme**
  - Merkle-Hellman
  - Iterated MH
  - Graham-Shamir
  - Chor-Rivest etc