Diffie-Hellman Protocol. (DH)

- Fix a finite cyclic group G of order n (e.g. $G = (\mathbb{Z}_p)^*$)
- Fix a generator g in G. ($e.g.$, $G = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$)

Alice		Bob
choose a random a in $\{1, \ldots, n\}$		choose a random b in $\{1, \ldots, n\}$
	$A = g^a \bmod p$ →	
	← $B = g^b \bmod p$	

$$B^a_{\bmod p} = (g^b)^a = \boxed{k_{AB} = g^{ab}_{\bmod p}} = (g^a)^b = A^b_{\bmod p}$$

Computational Diffie-Hellman (CDH)

- G: finite cyclic group of order n.
- CDH assumption holds if: $g, g^a, g^b \Rightarrow g^{ab}$.

For all efficient algorithms A:

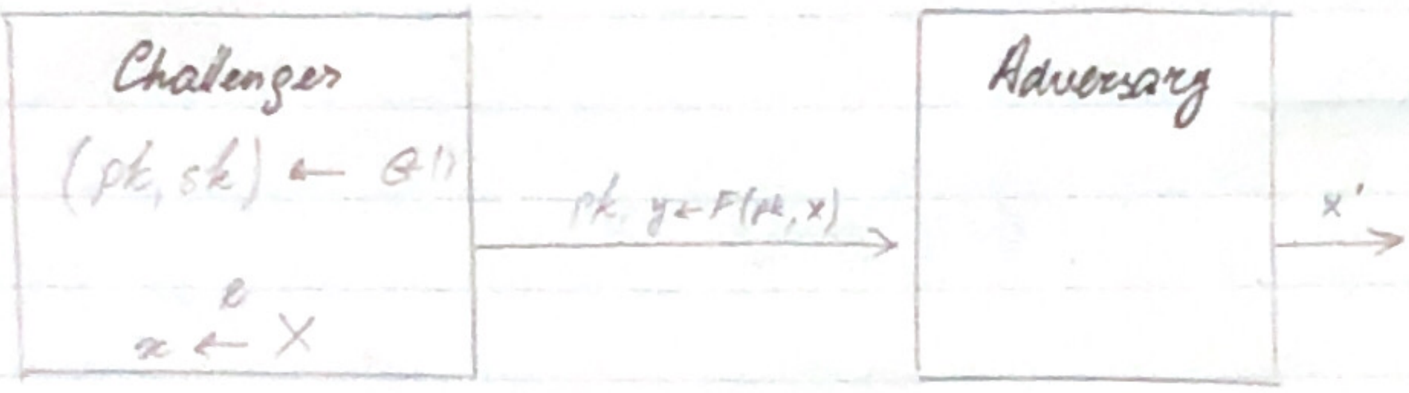
$$\Pr[A(g, g^a, g^b) = g^{ab}] < \text{negligible}$$

where $g \leftarrow$ { generators of G }
$a, b \leftarrow \mathbb{Z}_n$

- Some Trapdoor Permutations (TDP's) are constructed directly from CDH

Secure Trapdoor Functions (TDFs)

- (G, F, F^{-1}) is a secure TDF which can be evaluated but cannot be inverted without sk



Def: (G, F, F^{-1}) is a secure TDF if for all eff A:

$$Adv_{ow}[A, F] = P_2[x = x'] < negl.$$

- (G, F, F^{-1}) – secure TDF $X \to Y$.
- (E_s, D_s) – sym. auth. enc scheme over (K, M, C).
- $h : X \to K$ – a hash function.

$E(pk, m)$:

$x \leftarrow X$, $y \leftarrow F(pk, x)$

$k \leftarrow h(x)$, $c \leftarrow E_s(k, m)$

output (y, c)

$D(sk, (y, c))$:

$x \leftarrow F^{-1}(sk, y)$

$k \leftarrow h(x)$, $m \leftarrow D_s(k, c)$

output m

- Cannot apply F directly to plaintext (deterministic)
  - ↳ Incorrect. $E(pk, m)$: output $c \leftarrow F(pk, m)$

Arithmetic mod

- Let $N = pq$ where p, q are prime
- $Z_N = \{0, 1, 2, \ldots, N-1\}$ $\quad (Z_N)^* = \{$invertable elements in $Z_N\}$
- Fact $x \in Z_N$ is invertable iff $\gcd(x, N) = 1$.
- Num of elements in $(Z_N)^*$ is $\varphi(N) = (p-1)(q-1) = N - p - q + 1$

- Euler's theorem: $\forall x \in (Z_N)^* : x^{\varphi(N)} = 1$

RSA TDP

- $G()$: choose random primes $p, q \approx 1024$ bits.
  set $N = pq$.
  choose integers e, d such that $e \cdot d = 1 \pmod{\varphi(N)}$
  => output $pk = (N, e)$
  $sk = (N, d)$

generation algorithm

- $F(pk, x) : Z_N^* \to Z_N^*$; $RSA(x) = x^e \quad (\in Z_N)$
  compute trapdoor permutation

- $F^{-1}(sk, y)$; $y^d = RSA(x)^d = x^{ed} = x^{k\varphi(N)+1}$
  inverting the permutation $= (x^{\varphi(N)})^k \cdot x = 1 \cdot x = x$
  $k = 1$

Def. (RSA assumption) RSA is a one way permutation.

For all eff. algorithms A:

$$Pr[A(N, e, y) = y^{1/e}] < \text{negl.}$$

where $p, q \xleftarrow{R}$ n bit primes,
$N \leftarrow pq$
$y \leftarrow Z_N^*$ Yibin