

## 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.,  $G = \{1, g, g^2, g^3, \dots, g^{n-1}\}$ ).

Alice

choose a random  $a$  in  $\{1, \dots, n\}$

$$A = g^a \text{ mod } p$$

Bob

Choose a random  $b$  in  $\{1, \dots, n\}$

$$B = g^b \text{ mod } p$$

$$B^a \text{ mod } p = (g^b)^a = \boxed{k_{AB} = g^{ab} \text{ mod } p} = (g^a)^b = A^b \text{ mod } p$$

## 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  $A$ :

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

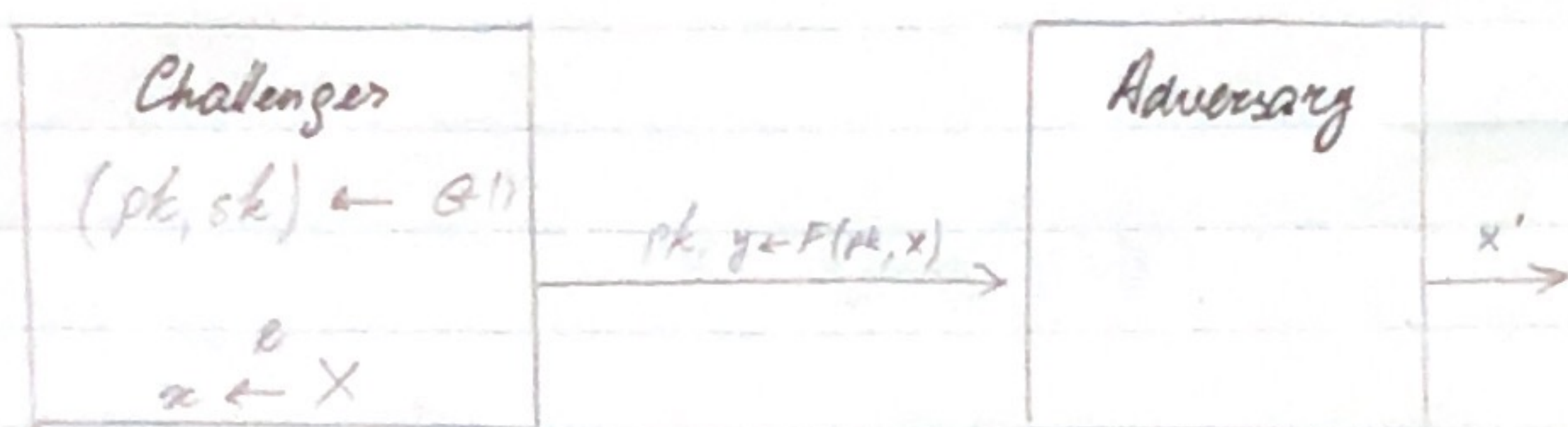
where  $g \leftarrow \{\text{generators of } G\}$   
 $a, b \leftarrow \mathbb{Z}_n$

- Some Trapdoor Permutations (TDPs) 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  $A$ :

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

- $(G, F, F^{-1})$  - secure TDF  $X \rightarrow Y$ .
- $(E_s, D_s)$  - sym. auth. enc scheme over  $(k, m, c)$ .
- $H: X \rightarrow K$  - 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).  
 $\hookrightarrow$  Incorrect:  $E(pk, m)$ : output  $c \leftarrow F(pk, m)$



## Arithmetic mod

- let  $N = p \cdot q$  where  $p, q$  are prime.
- $\mathbb{Z}_N = \{0, 1, 2, \dots, N-1\}$  ;  $(\mathbb{Z}_N)^* = \{\text{invertible elements in } \mathbb{Z}_N\}$
- Fact  $x \in \mathbb{Z}_N$  is invertible if  $\gcd(x, N) = 1$ .
- Num of elements in  $(\mathbb{Z}_N)^*$  is  $\phi(N) = (p-1)(q-1) = N - p - q + 1$
- Euler's theorem:  $\forall x \in (\mathbb{Z}_N)^* : x^{\phi(N)} = 1$

## RSA TDP

- $G()$ : choose random primes  $p, q \approx 1024$  bits.  
set  $N = pq$ .  
choose integers  $e, d$  such that  $e \cdot d = 1 \pmod{\phi(N)}$   
 $\Rightarrow$  output  $pk = (N, e)$   
 $sk = (N, d)$   
generation algorithm
- $F(pk, x) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$  ;  $RSA(x) = x^e \pmod{N}$   
compute trapdoor permutation
- $F^{-1}(sk, y)$  ;  $y^d = RSA(x)^d = x^{ed} = x^{1 + k\phi(N)} = (x^{\phi(N)})^k \cdot x = 1 \cdot x = x$   
inverting the permutation  
 $k = 1$

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  $p, q \xleftarrow{R} n\text{-bit primes}$   
 $N \leftarrow pq$   
 $y \leftarrow \mathbb{Z}_N^*$  choice