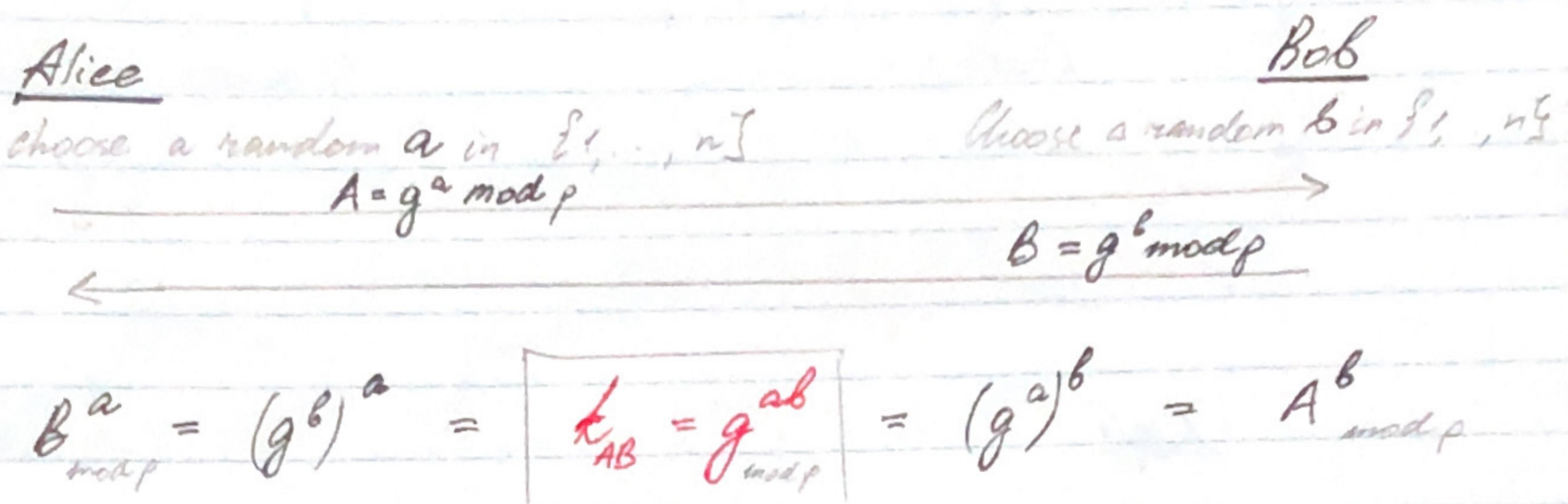


## Diffie-Hellman Protocol. (DH)

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



## Computational Diffie-Hellman (CDH)

- $G$ : finite cyclic group of order  $n$ .
- CDH assumption holds if:  $g, g^a, g^b \not\Rightarrow g^{ab}$ .

For all efficient algorithms  $A$ :

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

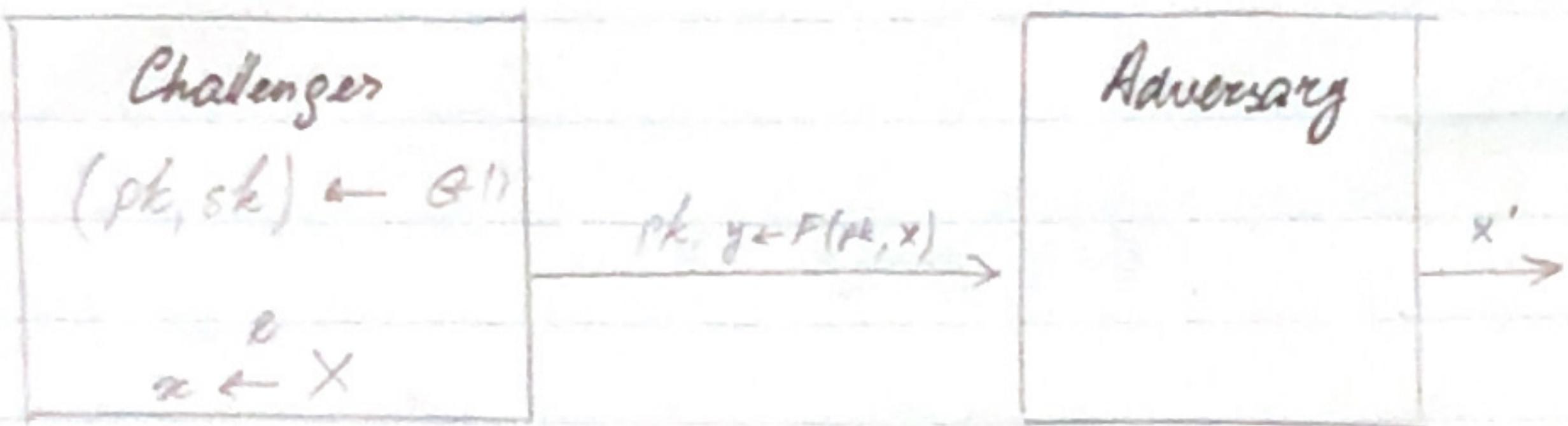
where  $g \leftarrow \{\text{generators of } G\}$   
 $a, b \leftarrow \mathbb{Z}_n$

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

Hilary

## Secure Trapdoor Functions (TDFs)

- $(G, F, F')$  is a secure TDF which can be evaluated, but cannot be inverted without  $sk$



Def:  $(G, F, F')$  is a secure TDF if for all off  $A$ :

$$\text{Adv}_{\alpha}[A, F] = \Pr_{\alpha}[x = x'] < \text{negl.}$$

- $(G, F, F')$  - secure TDF  $X \rightarrow Y$ .
- $(E_s, D_s)$  - sym. auth. enc. scheme over  $(k, m, c)$ .
- $H: X \rightarrow K$  - a hash function.

$E(pk, m)$ :

$$\begin{aligned} x &\leftarrow X, \quad y \leftarrow F(pk, x) \\ k &\leftarrow H(x), \quad c \leftarrow E_s(k, m) \\ \text{output } (y, c) \end{aligned}$$

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

$$\begin{aligned} x &\leftarrow F^{-1}(sk, y) \\ k &\leftarrow H(x), \quad m \leftarrow D_s(k, c) \\ \text{output } m \end{aligned}$$

- Cannot apply  $F$  directly to plaintext (deterministic).
- 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 iff  $\gcd(x, N) = 1$ .
- 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  $pk = (N, e)$   
 $sk = (N, d)$
- $F(pk, x) : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* ; RSA(x) = x^e \pmod{N}$   
compute leapdoor permutation
- $F^{-1}(sk, y) ; y^d = RSA(x)^d = x^{ed} = x^{\frac{\phi(N)+1}{e}} = (x^{\phi(N)})^k \cdot x = 1 \cdot x = x$   
inverting the permutation

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

For all off algorithms A:

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

where  $p, q \xleftarrow{R} n$ -bit primes,

$$N \leftarrow pq$$

$$y \leftarrow \mathbb{Z}_N^* \quad \text{uniform}$$