CSE 539: Applied Cryptography
RSA + DHKE + PK

Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap15.pdf

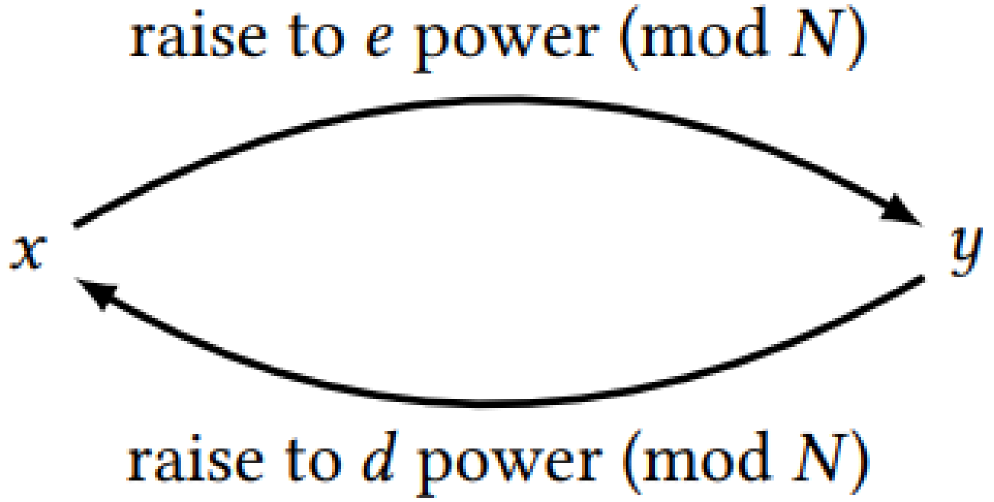
RSA

The RSA function is defined as follows:

- Let p and q be distinct primes (later we will say more about how they are chosen), and let $N = pq$. N is called the **RSA modulus**.
- Let e and d be integers such that $ed \equiv_{\phi(N)} 1$. That is, e and d are multiplicative inverses mod $\phi(N)$ — not mod N!
- The RSA function is: $x \mapsto x^e \,\%\, N$, where $x \in \mathbb{Z}_N$.
- The inverse RSA function is: $y \mapsto y^d \,\%\, N$, where $x \in \mathbb{Z}_N$.

RSA Security

- Given only the public information (N, e), it should be hard to compute the RSA inverse (y -> y^d mod N) on randomly chosen values.
  - In other words, the only person who is able to compute the RSA inverse function is the person who generated the RSA parameters



RSA Security

- But, if we know extra information about p and q, we can break RSA security
- For example, given $\delta = |p - q|$

RSA Security

- But, if we know extra information about p and q, we can break RSA security
- For example, given $\delta = |p^2 - q|$

RSA Security

- But, if we know extra information about p and q, we can break RSA security
- For example, given that p and q are close (e.g. $|p - q| < 1000$)

DHKE

Alice		Bob
$a \leftarrow \mathbb{Z}_n$	$A = g^a \ \%p \longrightarrow$	
	$\longleftarrow B = g^b \ \%p$	$b \leftarrow \mathbb{Z}_n$
return $B^a \ \%p$		return $A^b \%p$

Definition 14.2 (Discrete Log) *The* ***discrete logarithm problem*** *is: given $X \in \langle g \rangle$, determine a number x such that $g^x = X$. Here the exponentiation is with respect to the multiplication operation in $\mathbb{G} = \langle g \rangle$.*

Diffie-Hellman Key Agreement

- Quiz Sample:

Consider the following key-exchange protocol where p, g, q are public parameters

(i) Alice chooses a random exponent $a_1 \leftarrow \mathbb{Z}_q$ and computes $h_1 = g^{a_1} \bmod p$. Alice sends h_1 to Bob

(ii) Bob chooses two random exponents a_2, a_3, and computes $h_2 = g^{a_2+a_3} \bmod p$. Bob sends h_2 to Alice.

(iii) Alice outputs a shared key $k = h_2^{a_1} \bmod p$

Show how Bob outputs the same key k?

Diffie-Hellman Key Agreement

- Quiz Sample:

Consider the following key-exchange protocol where p, g, q are public parameters

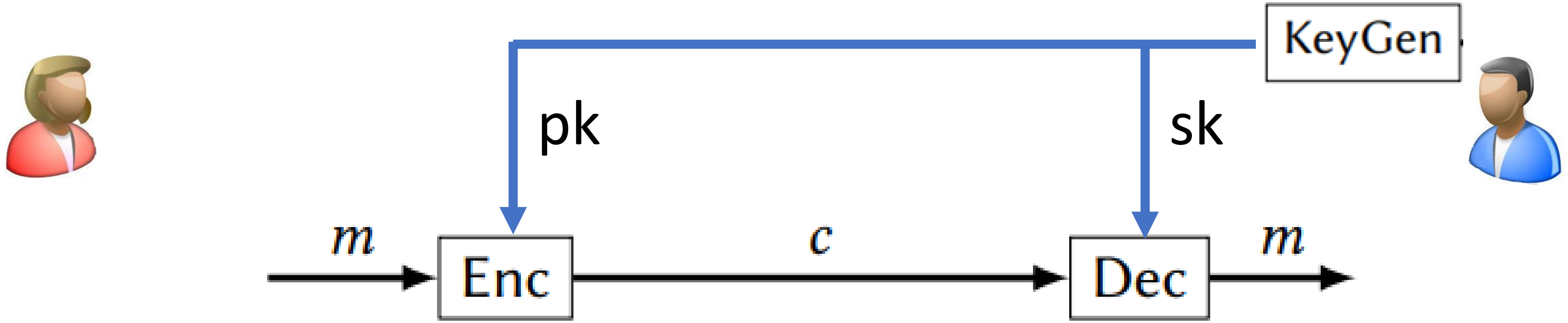
(i) Alice chooses a random exponent $a_1 \leftarrow \mathbb{Z}_q$ and computes $h_1 = g^{a_1} \bmod p$. Alice sends h_1 to Bob

(ii) Bob chooses two random exponents a_2, a_3, and computes $h_2 = g^{a_2+a_3} \bmod p$. Bob sends h_2 to Alice.

(iii) Alice outputs a shared key $k = h_2^{a_1} \bmod p$

Show how Bob outputs the same key k?

Public Key



Public Key: ElGamal Encryption

ElGamal encryption is a public-key encryption scheme that is based on DHKA. Given a choice of cyclic group $\mathbb{G}$ with n elements and generator g, the construction of ElGamal encryption is as below:

Keygen:	Enc($A, M \in \mathbb{G}$):	Dec($a, (B, X)$):
$sk := a \leftarrow \mathbb{Z}_n$	$b \leftarrow \mathbb{Z}_n$	return $X(B^a)^{-1}$
$pk := A := g^a$	$B := g^b$	
return (sk, pk)	return $(B, M \cdot A^b)$	

ElGamal Encryption

Suppose you do not know the secret key sk. Given the public key pk and the ElGamal ciphertext (B, X) that encrypts an unknown plaintext $M \in \mathbb{G}$, construct another ElGamal ciphertext (B', X') that decrypts to the same M (e.g., show how to do it without knowing M). Show the correctness of your construction.

ElGamal Encryption

Suppose you do not know the secret key sk. Given the public key pk and the ElGamal ciphertext (B, X) that encrypts an unknown plaintext $M \in \mathbb{G}$, construct another ElGamal ciphertext (B', X') that decrypts to M^2 (e.g., show how to do it without knowing M). Show the correctness of your construction.

ElGamal Encryption

Suppose you do not know the secret key sk. Given the public key pk and the ElGamal ciphertext (B, X) that encrypts an unknown plaintext $M \in \mathbb{G}$, construct another ElGamal ciphertext (B', X') that decrypts to M^2 (e.g., show how to do it without knowing M). Show the correctness of your construction.