CSE 539: Applied Cryptography
Week 8: Diffie-Hellman Key Agreement

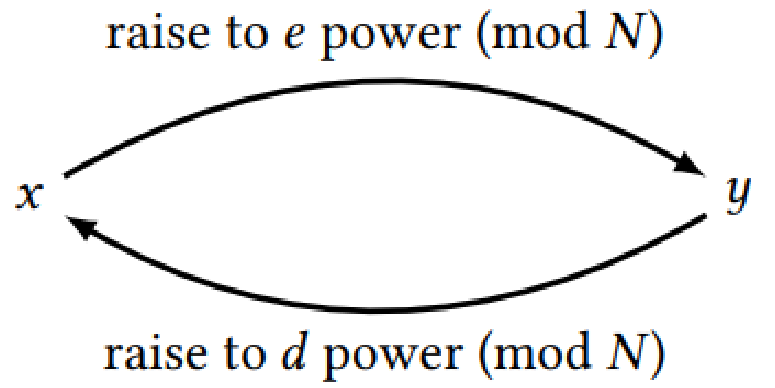
Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap14.pdf
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

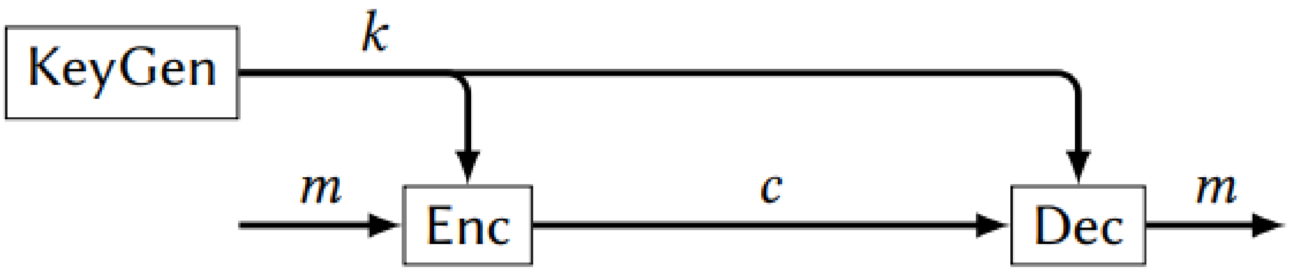
Recap: RSA

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 $x \in \mathbb{Z}_N$.



Recall: Encryption Basics & Terminology



- How to setup k?

Diffie-Hellman Key Agreement

- Introduced in 1976
- First practical method for establishing a shared secret over an unsecured channel

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

Diffie-Hellman Key Agreement

- Quiz Sample: In the execution of Diffie-Hellman key agreement, Alice and Bob use the prime p=23 and the primitive root g=11. Alice chooses the secret key a=6. Similarly, Bob chooses the secret key b=15. What is the Alice & Bob's shared key?

Cyclic Groups

Definition 14.1 *Let $g \in \mathbb{Z}_n^*$. Define $\langle g \rangle_n = \{g^i \% n \mid i \in \mathbb{Z}\}$, the set of all powers of g reduced mod n. Then g is called a* **generator** *of $\langle g \rangle_n$, and $\langle g \rangle_n$ is called the* **cyclic group generated by** *g* **mod** *n.*

If $\langle g \rangle_n = \mathbb{Z}_n^*$, then we say that g is a **primitive root mod** *n.*

Cyclic Groups

- Any cyclic group is closed under multiplication. That is, take any $X, Y \in \mathbb{G}$; then it must be possible to write $X = g^x$ and $Y = g^y$ for some integers x, y. Using the multiplication operation of $\mathbb{G}$, the product is $XY = g^{x+y}$, which is also in $\mathbb{G}$.
- Any cyclic group is closed under inverses. Take any $X \in \mathbb{G}$; then it must be possible to write $X = g^x$ for some integer x. We can then see that $g^{-x} \in \mathbb{G}$ by definition, and $g^{-x}X = g^{-x+x} = g^0$ is the identity element. So X has a multiplicative inverse (g^{-x}) in $\mathbb{G}$.

Diffie-Hellman Key Agreement

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?