Introduction to Cryptography

Liubov Slesarenko and Chloe Zhong

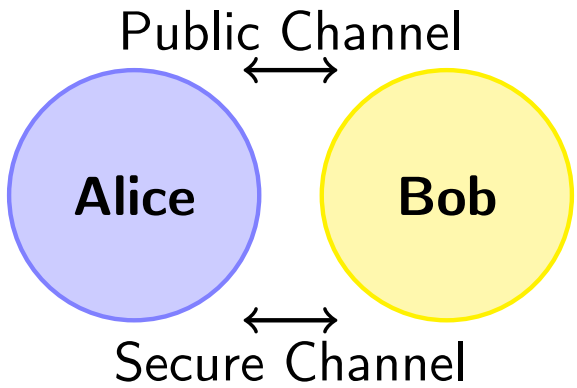
MIT PRIMES Circle

May 13, 2023

Overview

Get to Know Our Heroes:

- **Alice** and **Bob** are two fictional characters often used in cryptography to explain concepts and protocols.
- The goal of cryptography is to design protocols that allow Alice and Bob to communicate securely even if an eavesdropper, known as Eve, can intercept and manipulate their messages.
- Let's follow Alice and Bob as they use some of the most important cryptographic protocols!



Secret key encryption

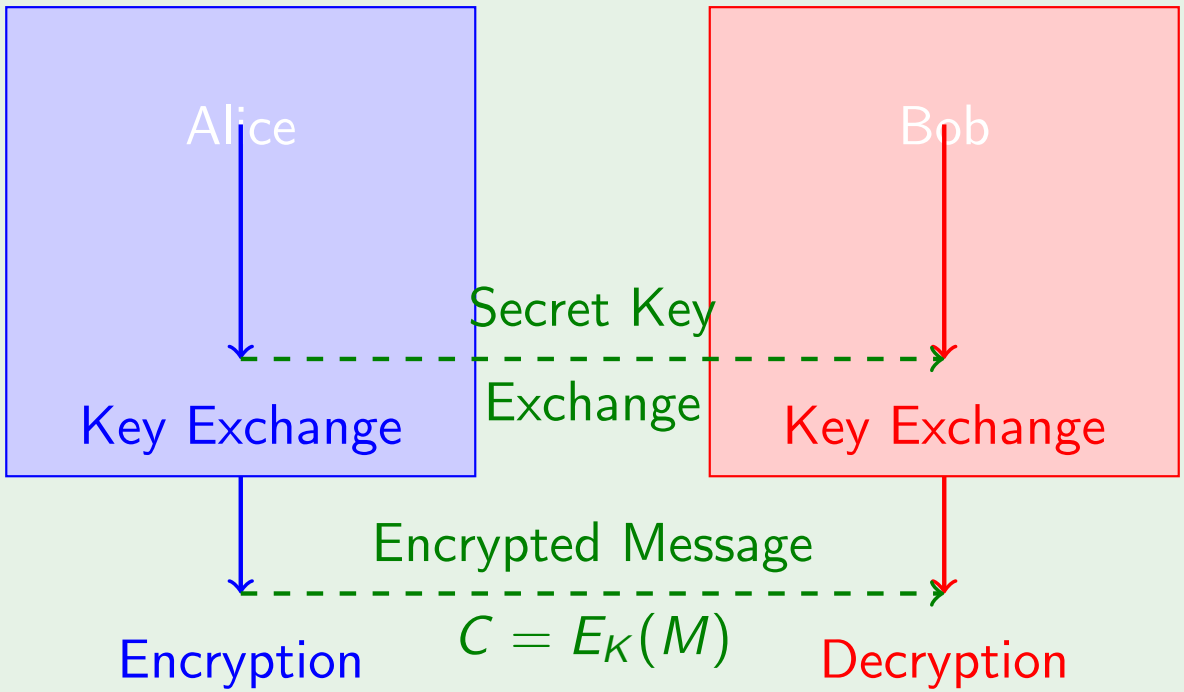
Definition

- Secret key encryption, also known as symmetric-key cryptography, is a cryptographic system that uses the same key for both encryption and decryption of data.
- The key is kept secret by the owner and is used to encrypt and decrypt messages.

Secure Communication with a Shared Key

Example

Alice wants to send a confidential message to Bob over the internet. Alice and Bob agree on a secret key and exchange it securely. Alice uses the key to encrypt the message and sends the encrypted message to Bob. Bob uses the same key to decrypt the message and read it. Only Alice and Bob can decrypt the message because they are the only ones who have access to the secret key.



The problem with secret key encryption

- But to share a secret key that Eve does not know, Alice and Bob have to meet in person!

The problem with secret key encryption

- But to share a secret key that Eve does not know, Alice and Bob have to meet in person!
- Imagine a world where every time you wanted to text someone, you had to meet them in person and share a secret key for communication between you two.

The problem with secret key encryption

- But to share a secret key that Eve does not know, Alice and Bob have to meet in person!
- Imagine a world where every time you wanted to text someone, you had to meet them in person and share a secret key for communication between you two.
- Public key cryptography comes to the rescue!

Public Key Cryptography

Definition

- Public key cryptography is a cryptographic system that uses a pair of keys, a *public key* and a *private key*, to encrypt and decrypt data.
- The public key is freely available to anyone who wants to send a message to the owner of the private key.
- Public key cryptography allows for secure communication over an insecure channel, such as the internet.

Fermat's Little Theorem

Suppose p is a prime number.

Theorem

For any integer x such that p does not divide x,

$$x^{p-1} \equiv 1 \mod p$$

Field $\mathbb{F}_p$ - What is it?

Definition

A field $\mathbb{F}_p$ is a set of integers modulo a prime p, with addition and multiplication defined modulo p. For example, let $p = 5$. Then, the elements of $\mathbb{F}_5$ are $\{0, 1, 2, 3, 4\}$, and we define the operations as follows:

- Addition: $a + b \equiv c \mod p$, where c is the remainder when $a + b$ is divided by p.
- Multiplication: $a \times b \equiv c \mod p$, where c is the remainder when $a \times b$ is divided by p.

$$\mathbb{F}_p \text{ is } \{0, 1, 2, ..., p-1\}$$

The discrete logarithm problem

Theorem

Let g be a primitive root for F_p and let h be a nonzero element of F_p. The Discrete Logarithm Problem (DLP) is the problem of finding an exponent x such that

$$g^x \equiv h(\mod p) \tag{1}$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$.

The discrete logarithm problem

Theorem

The discrete logarithm problem is a well-posed problem, namely to find an integer exponent x such that $g^x = h$. However, if there is one solution, then there are infinitely many because Fermat's little theorem tells us that $g^{p-1} \equiv 1 \pmod{p}$. Hence if x is a solution to $g^x = h$, then $x + k(p-1)$ is also a solution for every value of k, because

$$g^{x+k(p-1)} = g^x (g^{p-1})^k \equiv h \cdot 1^k \equiv h \pmod{p} \tag{2}$$

How hard is the discrete logarithm problem?

The task is to find x given g and h.

$$h = g^x$$
$$\log_g(h) = x$$

The problem is computationally hard since there is no known efficient algorithm to compute the discrete logarithm of h with respect to g.

- The DLP is believed to be computationally infeasible for sufficiently large keys, even with the best-known algorithms.
- The best-known algorithms for solving the DLP have exponential time and space complexity.

Diffie-Hellman Key Exchange

Example

Alice		**Bob**
Pick random a		Pick random b
$A \leftarrow g^a \pmod{p}$		$B \leftarrow g^b \pmod{p}$
	$A \longrightarrow$	
	$\longleftarrow B$	
$k_A \leftarrow A^a \pmod{p}$		$k_B \leftarrow B^b \pmod{p}$
$k_A = g^{ab} \pmod{p}$		$k_B = g^{ab} \pmod{p}$

Conclusion

- We explored that the Diffie-Hellman key exchange protocol has been presented as a fundamental algorithm in cryptography that enables public-key encryption.
- Our work builds up to this cryptosystem by discussing secret-key encryption and introducing necessary tools in number theory, and group theory. The discrete logarithm problem is also discussed, which is a critical aspect of the security of the Diffie-Hellman protocol.

References and Acknowledgements

References:

[1] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. *Undergraduate Texts in Mathematics* 2014.

Acknowledgements:

Thank you, Aparna, Mary, and Marisa, for all that you have done for us! We look forward to continuing our journey in math and hope to collaborate with you in the future.