CRYPTOSYSTEMS

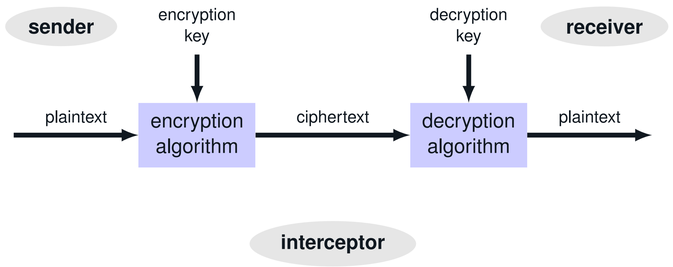
William Kim and Alex Giang

Virginia Tech

Introduction

A cryptosystem is a pair of algorithms that take a key and convert plaintext to ciphertext and back. In other words, a cryptosystem converts ordinary text into encrypted information that can be deciphered.

These systems are used for enhanced security systems, discrete messages over the internet, military communication, and commerce.



Cryptosystems are important in today's society. They provide user security and confidentiality all the way from military personnel to the average civilian. Examples include:

- Communication in the military
- Electronic transactions
- Password safety

Without Cryptosystems, the privacy of many people would be compromised.

Types of Cryptosystems

There are many types of cryptosystems, such as:

- Elliptic Curve - public key encryption technique that can be used to create faster, smaller, and more efficient cryptographic keys; used heavily in number theory.
- Diffie-Hellman - Allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.
- RSA - Used to encrypt and decrypt messages using two different keys.

Today, we will be focusing on Diffie–Hellman key exchange.

Diffie-Hellman Cryptographic Explanation

*Note: A number g is a primitive root modulo of n if for every integer x coprime to n, there is an integer k such that,

$$g^k \equiv a \pmod{n}.$$

Suppose there are three people, Alice, Bob, and Eve. Alice and Bob are trying to exchange information while Eve is simply an onlooker from the outside. To begin, Alice and Bob must first publicly agree to two numbers, p and g, where p is a prime number and g is a primitive root modulo p.

Alice		Bob		Eve	
Known	**Unknown**	**Known**	**Unknown**	**Known**	**Unknown**
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	

After this, Alice and Bob must each choose their own secret numbers, otherwise known as keys.

$a = 6$	b	$b = 15$	a		a, b

With their secret numbers, Alice and Bob must now calculate A and B respectively.

$A = 5^6 \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			

Once Alice and Bob calculate their respective values, they then publicly swap values and then repeat the same process, this time using the new integer values that they received instead of g. After this calculation, both Alice and Bob should arrive at the same solution, otherwise known as the shared secret key. It is important to note that even though Eve is able to see p, g, A, and B, in a practical aspect where p is much larger, it would be extremely time consuming and computationally expensive to run through all of the possible outcomes.

$B = 19$		$A = 8$		$A = 8$, $B = 19$	
$s = B^a \bmod 23$		$s = A^b \bmod 23$			
$s = 19^6 \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$			s

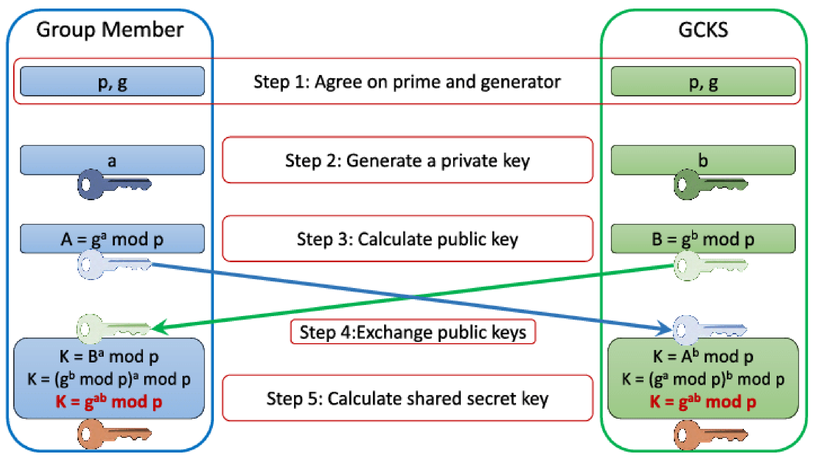


Fig. 5: Secrecy Chart [2]

Security issues

- Many services that use DH Key exchange often use the same prime numbers, which leaves itself vulnerable to algorithmic attacks.
- Keys used in a cryptosystem may be lost; the encrypted date inside of the lost key may be permanently lost.
- Backdoors implanted by state actors, such as the NSA, provide an easy way in without the use of brute force.

Security issues such as these may lead to:

- Invasion of privacy
- Permanent loss of sensitive data
- Theft

Future Research

This topic is important for future research because security and privacy is used by billions everyday; we should continue to research and improve cryptosystems so that our confidentiality will remain protected in the future.

Questions we would like to research in the future

- How can we make cryptosystems more secure?
- Where else can be cryptosystems be applied?
- How many other types of cryposystems are there and how do they differ?

sources

[1] National Research Council. *Cryptography's Role in Securing the Information Society*. The National Academies Press, 1996. ISBN: 978-0-309-05475-1. DOI: 10.17226/5131.

[2] *Design and Implementation of Security Gateway for Synchrophasor Based Real-Time Control and Monitoring in Smart Grid*. https://ieeexplore.ieee.org/document/7961134. June 2017.

[3] *Diffie Hellman Key Exchange*. https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange#cite_note-9. May 2020.

[4] *Plaintext Definition*. www.linfo.org. Apr. 2020.

[5] Sarah Simpson. *Cryptography in Everyday Life*. http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html. Apr. 2020.

[6] Martin E. Hellman Whitfield Diffie. *New Directions in Cryptography*. https://ee.stanford.edu/~hellman/publications/24.pdf. Nov. 1976.