Cryptography

**Introduction [1]**

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages. And so we begin.

What is cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Encryption and decryption

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to make sure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption. The following figure shows this process.

Means dif to dif ppl, key & cypher, threat models, kerckhoff’s princ.

***Relevant techs/apps***

*Filler here*

* *Secure storage*

*Filler here*

* + *Hash nd salt*
* Secure communication

Filler here

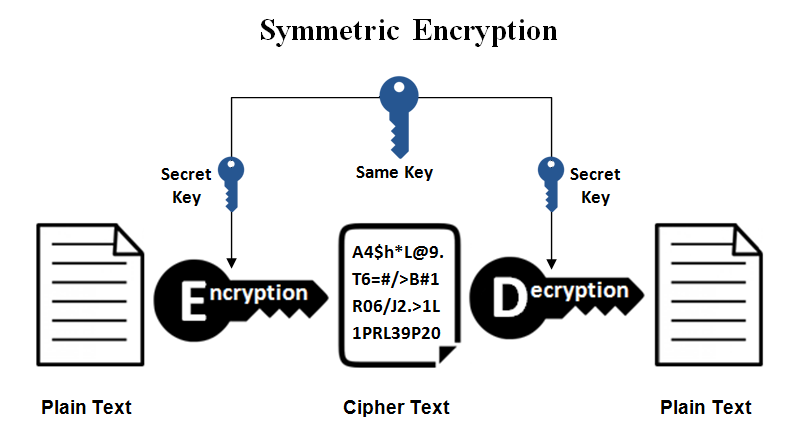
* + Methods/types

Filler here

* + - Symmetric

[3]

**What is Symmetric Encryption?**



This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetric encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

[2]

The question of key exchange was one of the first problems addressed by a cryptographic protocol. This was prior to the invention of public key cryptography. The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key

**Diffie-Hellman Algorithm**

Steps in the algorithm:

1 Alice and Bob agree on a prime number p and a base g.

2 Alice chooses a secret number a, and sends Bob ( g a mod p).

3 Bob chooses a secret number b, and sends Alice ( g b mod p).

4 Alice computes (( g b mod p ) a mod p).

5 Bob computes (( g a mod p ) b mod p).

Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

**Diffie-Hellman Example**

1. Alice and Bob agree on p = 23 and g = 5.

2. Alice chooses a = 6 and sends 5 6 mod 23 = 8.

3. Bob chooses b = 15 and sends 515 mod 23 = 19.

4. Alice computes 19 6 mod 23 = 2.

5. Bob computes 815 mod 23 = 2.

Then 2 is the shared secret. Clearly, much larger values of a, b, and p are required. An eavesdropper cannot discover this value even if she knows p and g and can obtain each of the messages

**Diffie-Hellman Security**

Suppose p is a prime of around 300 digits, and a and b at least 100 digits each. Discovering the shared secret given g, p, g a mod p and g b mod p would take longer than the lifetime of the universe, using the best known algorithm. This is called the discrete logarithm problem.

**Attacks on Diffie-Hellman**

• This is key exchange, not authentication.

– You really don’t know anything about who you have exchanged keys with

– The man in the middle …

– Alice and Bob think they are talking directly to each other, but Mallory is actually performing two separate exchanges

• You need to have an authenticated DH exchange

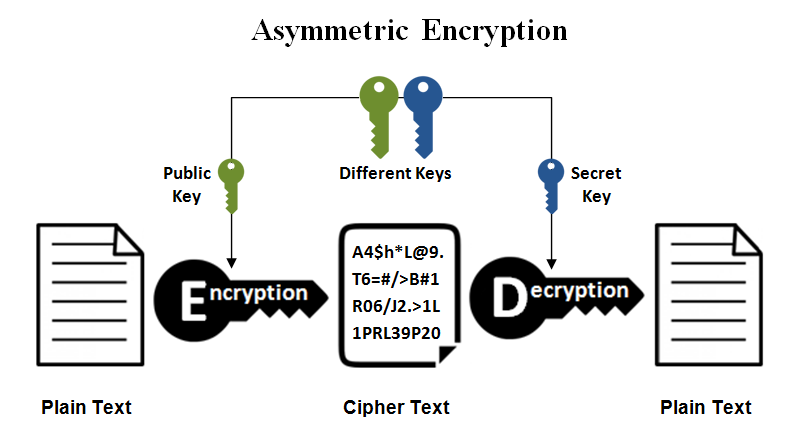
– The parties sign the exchanges (more or less)

– See Schneier for a intuitive description

* + - Asymmetric

[4]

**What is Asymmetric Encryption?**



Asymmetric encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetric encryption uses two related keys to boosting security. A [public key](https://www.ssl2buy.com/wiki/what-is-a-public-and-private-key-pair/) is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes EIGamal, [RSA, DSA, Elliptic curve techniques](https://www.ssl2buy.com/wiki/ecc-algorithm-to-enhance-security-with-better-key-strength/), PKCS.

* + - * RSA
      * SSL

**Conclusion**

**Drafts: no writing**

Doc draft

Script draft

Ppt draft

1: <https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf>

2: <http://www.cse.psu.edu/~trj1/cse497b-s07/slides/cse497b-lecture-6-cryptography.pdf>, https://www.cs.utexas.edu/~byoung/cs361/lecture52.pdf

3,4: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences