Cryptography

Salim Arfaoui

Lets Set Some Expectations

- We won’t be talking about cryptocurrency!
- Understanding of:
  - Crypto basics.
  - Types of crypto techniques.
  - Popular cryptosystems
  - Java and C++ implementation

- https://threatmap.checkpoint.com/

What is Cryptography?

Derived from the Greek word ***kryptos***, which means **hidden**.

CRYPTO + **GRAPHY** = secret writing

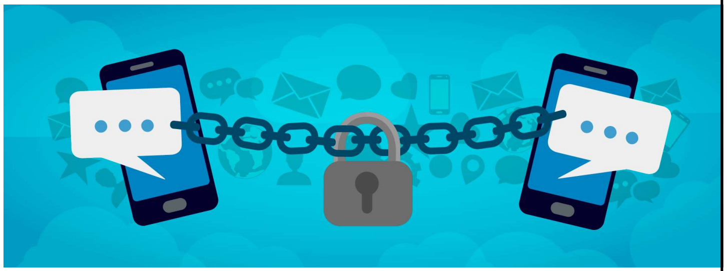
Cryptography is the study of **secure communications** techniques that allow **only** the sender and intended recipient of a message to view its contents.

-Kaspersky

Main Goals of Cryptography

Modern cryptography goals:

- **Confidentiality**
- **Data integrity**
- **Non-repudiation**
- **Authentication**



Confidentiality

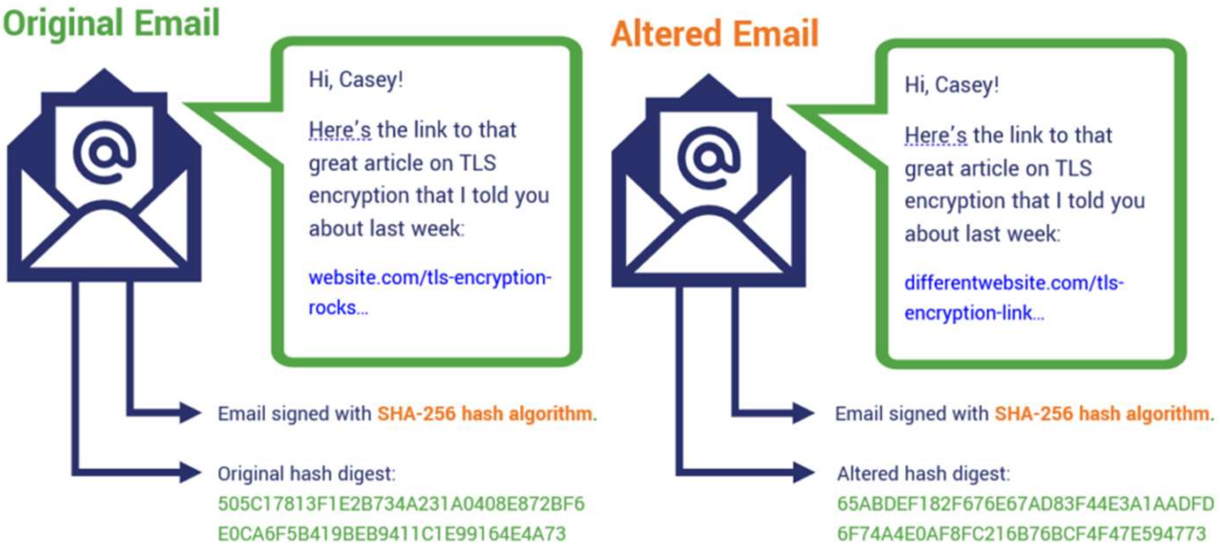
The act of **protecting data** against unlawful, unintentional, or unauthorized access, theft, or disclosure.

- The message is concealed by **encoding** it.
- The sender **encrypts** the message using a **cryptosystem**.
- The recipient **decrypts** the message using same cryptosystem.

Data Integrity

The act of **securing data** and information from unauthorized change, damage, or manipulation.

- Uses hashing to generate a unique message digest from the original message.
  (e.g., MD2, MD4, MD5, and Secure Hash Algorithm – 1).
- Recipient uses the same technique to generate a second digest from the message to compare to the original one.



Hi, Casey!

Here's the link to that great article on TLS encryption that I told you about last week:

website.com/tls-encryption-rocks...

Email signed with SHA-256 hash algorithm.

Original hash digest:
505C17813F1E2B734A231A0408E872BF6
E0CA6F5B419BEB9411C1E99164E4A73

Hi, Casey!

Here's the link to that great article on TLS encryption that I told you about last week:

differentwebsite.com/tls-encryption-link...

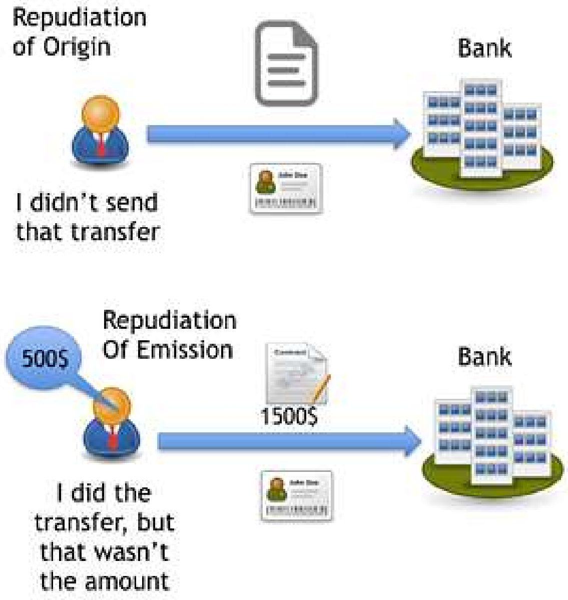
Email signed with SHA-256 hash algorithm.

Altered hash digest:
65ABDEF182F676E67AD83F44E3A1AADFD
6F74A4E0AF8FC216B76BCF4F47E594773

Non-repudiation

Senders cannot deny their intentions in the transmission of the information at a later stage.

Digital signatures can offer non-repudiation when it comes to online transactions.


Repudiation of Origin
Bank
I didn't send that transfer
Repudiation Of Emission
500$
Bank
1500$
I did the transfer, but that wasn't the amount

Authentication

- The act of **verifying the identities** of both the sender and the receiver of the information, such as the user or system.
- Popular authentication protocols:
  - **SSH** — a simple & useful security protocol
  - **SSL** — practical security on the Web
  - **IPSec** — security at the IP layer
  - **Kerberos** — symmetric key, single sign-on
  - **WEP** — "Swiss cheese" of security protocols
  - **GSM** — mobile phone (in)security

Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - deciphering *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

Types of cryptographic techniques

Three types of cryptographic techniques used in general:

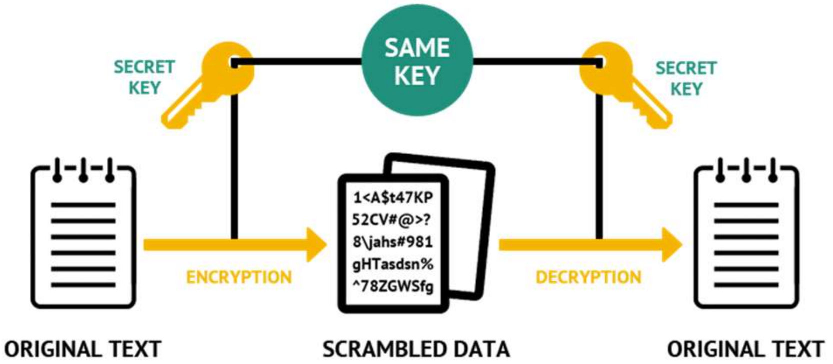
- **Symmetric Key Cryptography**
- **Asymmetric Key Cryptography**
- **Hash Function**

Symmetric Key Cryptography

The **single common key** is used by both sender and receiver for the purpose of encryption and decryption of a message.

Major drawback: Key exchange.

Types: AES (Advanced Encryption Standard), RC4, Blowfish, Stream ciphers, Block ciphers, etc.



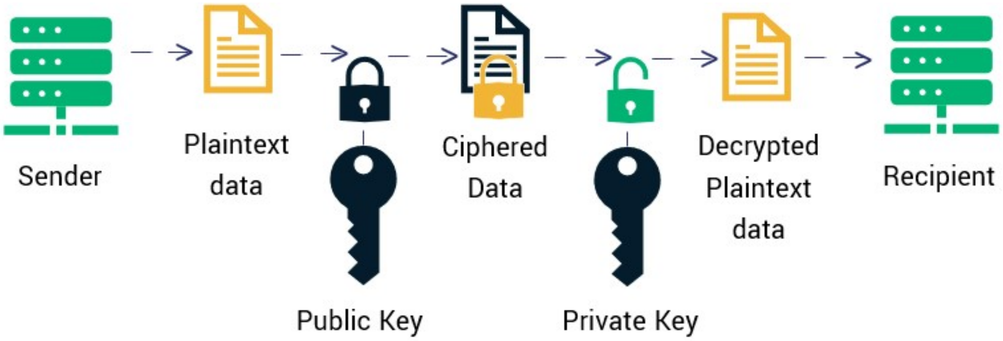
Asymmetric Key Cryptography

Two related keys **(public and private key)** are used.

- Public key is used for encryption
- Private key is used decryption.

Public key may be freely distributed, while its paired private key, remains a secret.

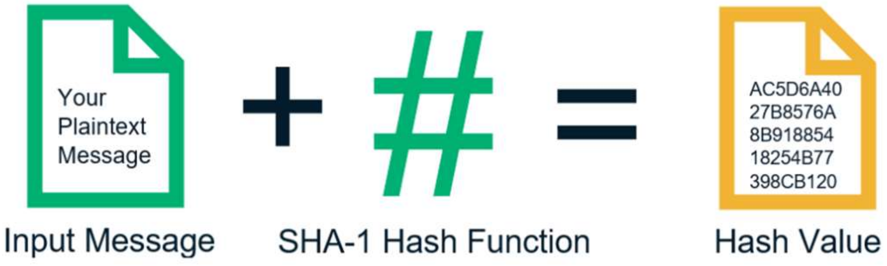
Types: Diffie Hellman, RSA, DSA, PKCs, etc.



Cryptographic Hash Functions

A one-way cryptographic algorithm that maps an input of any size to a unique output of a fixed length.

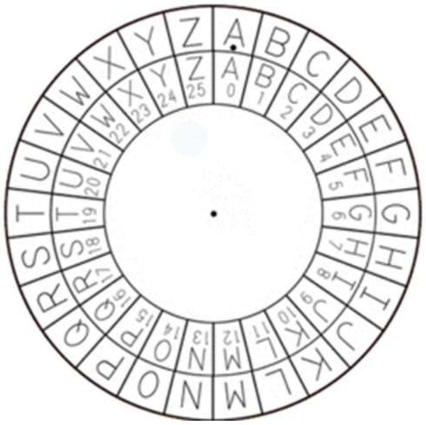
Examples: MD5, SHA Secure Hash Algorithm, RIPEMD, Whirlpool, etc.

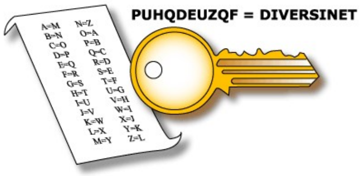


Caesar Cipher

Substitution Cipher / Shift cipher

Units of plain text are replaced with cipher text.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



Encryption:

Plaintext: Attack at dawn
Key: 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ciphertext?

Decryption:

Ciphertext: UHWXUA WR URPH
Key: 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Plaintext?

Rail-fence Cipher

Transposition cipher. Involves the rearranging of the letters in the plaintext to encrypt the message.

Rail-fence Cipher

Encryption Algorithm:

1. Grid (Rows / cols)
2. Rows = Key
3. Cols = number of Chars
4. Mark Zigzag pattern and place chars
5. Read chars one row at a time

Decryption Algorithm:

1. Grid (Rows / cols)
2. Rows = Key
3. Cols = number of Chars
4. Mark Zigzag pattern
5. Place chars one row at a time.
6. Read chars following the zigzag pattern

Encryption:

1. Grid (Rows / cols)
2. Rows = Key
3. Cols = number of Chars
4. Mark Zigzag pattern and place chars
5. Read chars one row at a time

Plaintext: defend the east wall
Key: 4

Ciphertext?

Decryption:

1. Grid (Rows / cols)
2. Rows = Key
3. Cols = number of Chars
4. Mark Zigzag pattern
5. Place chars one row at a time.
6. Read chars following the zigzag pattern

Ciphertext: HPe$eeloollp
Key: 4

Plaintext?

Caesar Cryptosystem in Java

Caesar Cryptosystem in C++