

Cryptography 101



Note: Moving forward we the students will NOT be using the Piazza platform

All students will be taken off.

Piazza will be strictly used for teachers and community supervisors

If you have any questions please take them to your teacher/community supervisor and they will reach out to a mentor to answer your question

Overview of Cryptography 101

- What is Cryptography
- Importance of Cryptography
- Encryption Algorithms
- History of Cryptography
- Substitution Ciphers
- Transposition Ciphers
- BREAK + GAME
- Symmetric Encryption
- Asymmetric Encryption
- Hashing

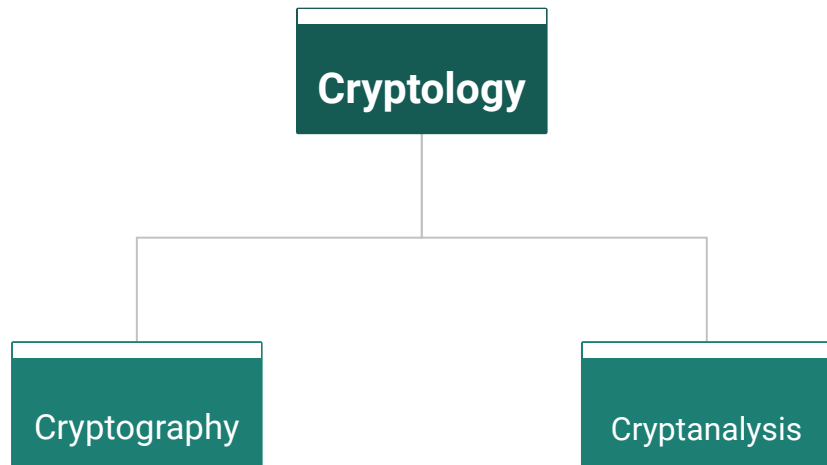


What is Cryptography?

Cryptography- Encrypting data from plaintext to ciphertext so that it can only be read by the intended recipient(s) and decrypting data from ciphertext to plaintext.

Cryptanalysis- Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. ([Searchsecurity.techtarget.com](https://searchsecurity.techtarget.com))

Cryptology- the scientific study of cryptography and cryptanalysis (Merriam Webster)



Importance of Cryptography

The background features a dark blue gradient with glowing, translucent blue lines of binary code (0s and 1s) swirling and looping around the central text area. In the center, behind the text box, is a faint, light blue shield icon with a keyhole at the bottom, symbolizing security and protection.

1. **Confidentiality:** Ensure that the data can only be seen by the intended recipients.
2. **Integrity:** Ensure that the received data has not been altered or tampered with.
3. **Non-repudiation:** Ensure that the sender really did send the data.
4. **Authentication:** The process of proving one's identity.

Important Terms

Plaintext - Original text, readable by human beings, something that we can understand

Ciphertext - Text after it has been encrypted

Cipher - An algorithm/technique for performing encryption or decryption

Encryption - The process of converting plaintext into ciphertext

Decryption - The process of converting ciphertext back into plaintext

Important Terms

Keys - A string used in combination with a cipher (encryption algorithm) to transform plaintext into ciphertext, without knowing the key ciphertext cannot be converted back to plaintext

Key space - Number of possible keys that can be created from an algorithm, the larger the key space the more secure the algorithm

Encryption Algorithms

Kerckhoffs' Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

An encryption algorithm is a mathematical formula used to transform data into meaningless ciphertext.

Use protocols and algorithms that are widely-used, heavily analyzed, and accepted as secure.


Longer the key size, the harder it is to brute force. However the larger the key size the more computing power is required.

Commonly used encryption algorithms include:

- DES
- AES - 128, 192, 256 bits in key size
- RSA

Block Cipher

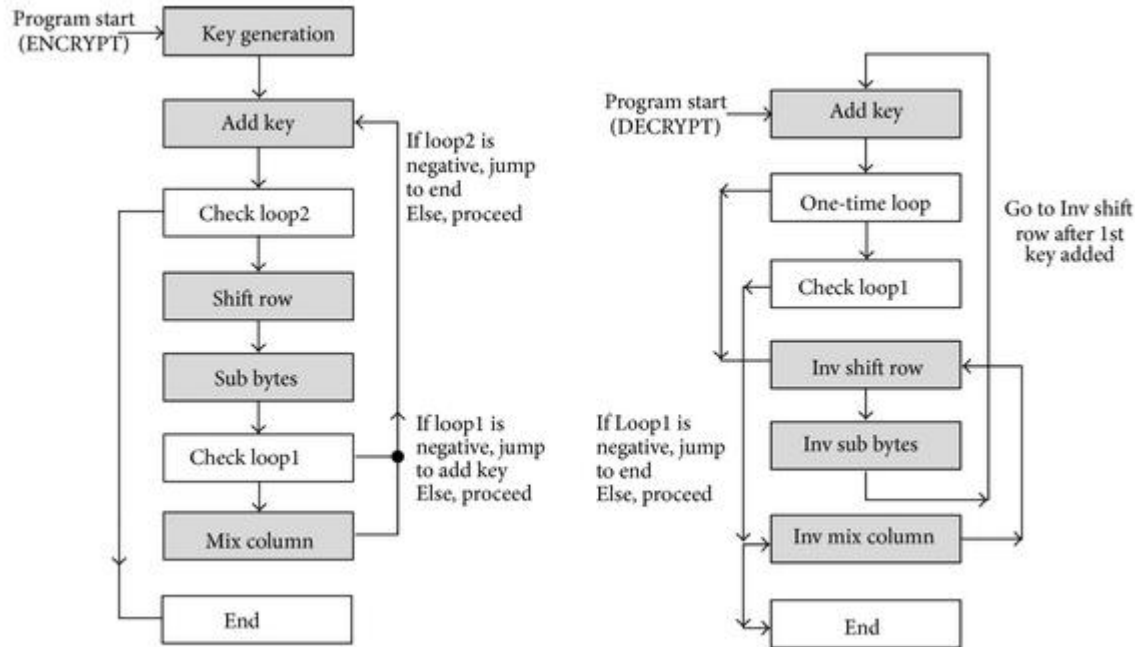
Encryption happens on a block of data

- 
- DES
 - 3DES
 - AES

Stream Cipher

Single bit of data is encrypted at a time

- 
- RC4
 - SEAL



Picture Source: Malwarebytes

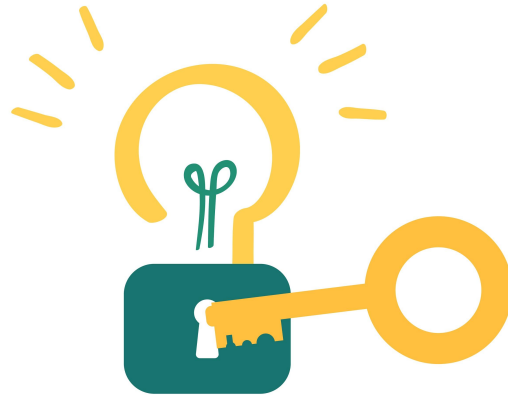
Encryption

Decryption

Plain text

Cipher text

Plain text



History of Cryptography

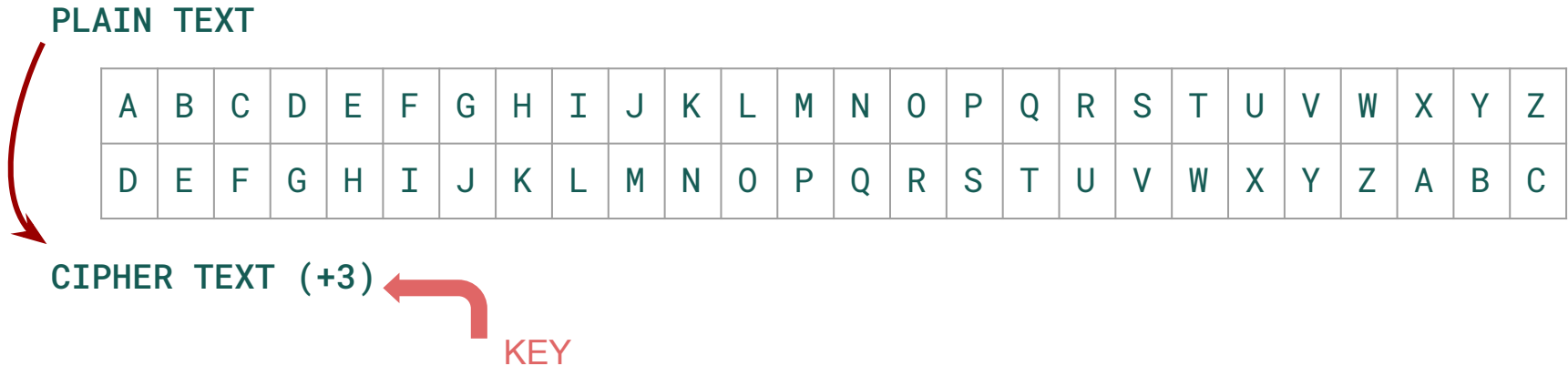
'Crypto' means hidden and 'graphy' means writing, so cryptography literally translates to **hidden writing**.

1900 B.C, Egyptians communicated secret messages using hieroglyphs, the code was only known to the scribes

100 B.C, Julius Caesar came up with a way to communicate with his army generals using a secret code. Now known as the Ceaser Cipher

Caesar Cipher

- Substitution Cipher
- Substitute one letter of the alphabet for another



ROT 13

- "Rotate by 13 places"
- Substitution cipher that replaces a letter with the 13th letter after it in the alphabet.

PLAIN 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
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

ROT 13

Vigenere Cipher

The Vigenère cipher uses a 26×26 table with A to Z as the row and column.

Ex. I LOVE CRYPTOGRAPHY

Key: CANHACKCANHACKCAN

Ciphertext: K LBCE EBAPGVGTRHL

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

Transposition Ciphers

Order of letters is rearranged according to a predetermined method.

Ex. Thisisasecretmessage

T	s	r	s
h	a	e	s
i	s	t	a
s	e	m	g
i	c	e	e

Ciphertext:
Tsrshaesistasemgicee

Key??

GAME
TIME

There are a few imposters here who are trying to eavesdrop on our conversation.

I am going to encrypt a message and send it to everyone.

The imposter is going to steal the data and see if they can decrypt the secret message.



Cipher: Ceasar Cipher

Key (+8)

Ciphertext: Ummb bwvqopb ib
amdmbv jg bpm amkzmb lwwz



Symmetric Encryption

- One key is used to encrypt plaintext and decrypt it as well
- The key is shared among the receiver and sender of data
- Key must be protected
- Ex. Caesar cipher, AES, DES



Asymmetric Encryption

- Also known as ‘public key cryptography’
- Involves a key pair that are mathematically connected and work in conjunction with each other
- Private key, public key (Key pair)
- The sender uses the receiver's Public key to encrypt the data and the private key is used by the receiver to decrypt the message.
- Ex. RSA, ECC, El Gamal



Hashing

- Hashing algorithms are one way algorithms and cannot be reversed.
- They create a unique 'hash' for the data
- Used to ensure integrity of data and to store passwords
- Popular hashing algorithms: MD5, SHA-1, SHA-2

Summary of Learnings

- Cryptography is used to provide confidentiality and protect private data
- Encryption converts plaintext into ciphertext which can only be decrypted by the intended recipients
- Keys are what makes encryption secret and must be protected
- Transposition ciphers vs Substitution Ciphers
- Symmetric Encryption vs Asymmetric Encryption
- Hashing used for Integrity

Resources

Resource Hub available at <https://dmz.ryerson.ca/canhack/>

PicoCTF primer available at <https://picoctf.org>

Online Tools for encrypting/decrypting:

<https://cryptii.com/>

<https://gchq.github.io/CyberChef/>

Thank you for your time!

Questions?

See you next week for Digital Forensics 101!

