

# CRYPTO & STEGANO

Mari berteman dengan anak-anak graphy



The background is a solid light orange color. There are three stylized orange clouds of varying sizes and shapes floating in the upper half. At the bottom, there are two stylized dark orange foliage sprigs, one on the left and one on the right, with multiple pointed leaves. The overall aesthetic is minimalist and modern.

# GET READY!

sebelum lanjut, bikin kopi dulu sabi lah...

# CRYPTO- GRAPHY

seni menjaga keamanan pesan.



# Naon Cryptography teh?

Bayangkan ketika seseorang ingin mengirimkan sebuah pesan rahasia, misalkan A ingin mengirimkan pesan ke si B, dan ada si C yang ingin mengetahui pesan tersebut. Untuk menghindari kebocoran informasi ke si C maka cryptography dibutuhkan..

**Enkripsi** : suatu proses mengubah pesan biasa (plain text) menjadi pesan yang tidak bisa dibaca (cipher text)

**Dekripsi** : suatu proses mengubah pesan yang tidak bisa dibaca (cipher text) menjadi pesan biasa (plain text)

**Cipher** : Suatu algoritma untuk melakukan enkripsi dan dekripsi



## Ciphers vs Codes

Code yaitu memetakan dari sesuatu yang memiliki makna seperti kata, kalimat, atau frase menjadi sesuatu yang lain.

<b>Accessory,</b>	Cannot sail by steamer you name. Will cable when steamer and date of departure are fixed.
<b>Accidental,</b>	Cannot say when shall be able to leave ——
<b>Acclimate,</b>	Cannot you start before ——
<b>Accordion,</b>	Cannot you start so as to reach here ——
<b>Accosted,</b>	Can you send me letter of introduction to ——
<b>Accountant,</b>	Come at once. Do not delay.
<b>Accretion,</b>	Care of ——
<b>Accumulate,</b>	Care of E. A. Adams & Co., Boston.
<b>Accurate,</b>	Care of Baring Bros. & Co., Liverpool.
<b>Accursed,</b>	Care of Baring Bros. & Co., London.
<b>Accusation,</b>	Care of Brown Brothers & Co., Boston.
<b>Accusing,</b>	Care of Brown Brothers & Co., New York.
<b>Accustom,</b>	Care of Brown, Shipley & Co., Liverpool.
<b>Acerbity,</b>	Care of Brown, Shipley & Co., London.



## Ciphers vs Codes

**Codebook** adalah daftar simpel dari sebuah pemetaan. Codebook harus sudah ada sejak pesan mulai ditulis. Cukup diingat, sebuah kode membutuhkan codebook.

**Cipher** tidak melibatkan makna apapun, tetapi menggunakan operasi secara mekanis yang kita sebut sebagai algoritma yang merubah baik suatu huruf maupun potongan huruf.

Contohnya pada Caesar cipher kita melihat suatu huruf dipetakan ke huruf lain. misal ketika kita menggunakan geser 3 : A→D, B→E, dan C→F





## Encoding?

Encoding adalah mengkodekan informasi dalam bentuk lain. Jika encoding ini tujuannya untuk menyembunyikan sesuatu maka disebut enkripsi.

## Base64

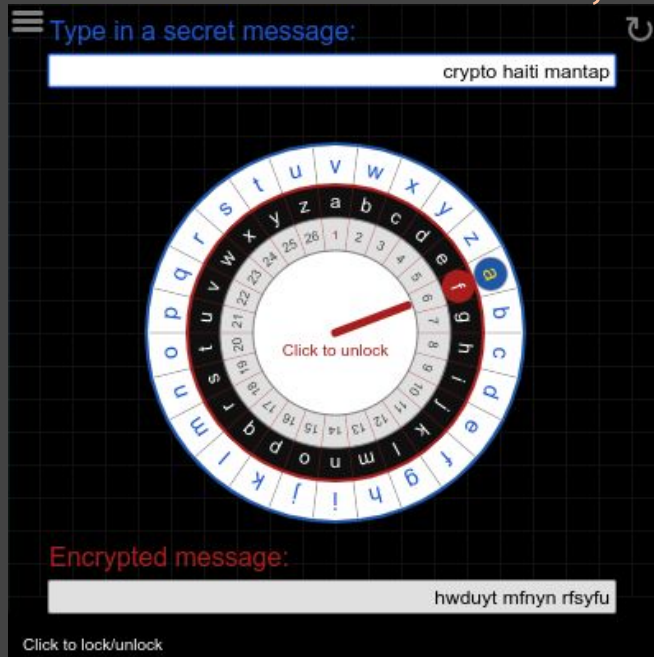
Base64 digunakan untuk mengubah representasi biner menjadi teks



# Caesar Cipher

Caesar cipher atau caesar shift adalah sebuah algoritma cipher yang menggunakan urutan / susunan alfabet dalam encoding teksnya.

Contoh Caesar dengan shift (pergeseran) 5:



ROT 13 sama saja dengan cipher, hanya saja shift yang digunakan harus 13

## Encryption: Caesar cipher

Shift over the alphabet a certain number of places & substitute the original letters for the shifted letters

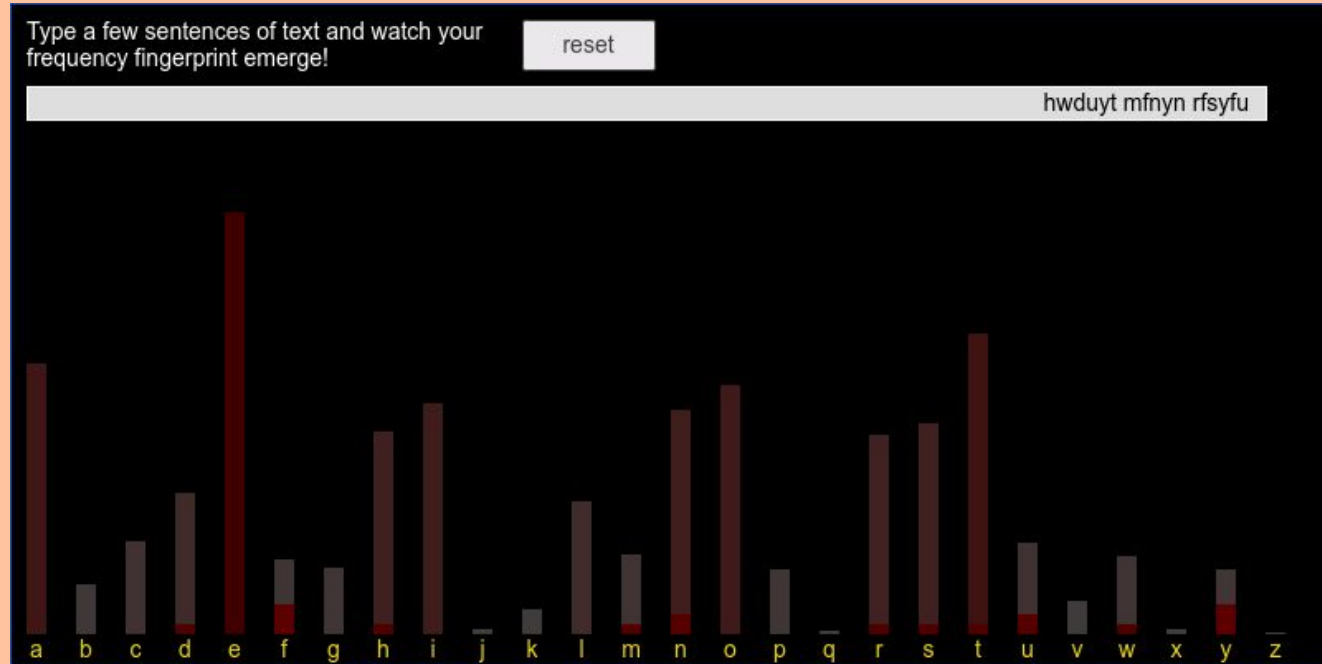
ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNOPQRSTUVWXYZABCDEFGHIJKL

HI WORLD	→	TU IADXP
----------	---	----------



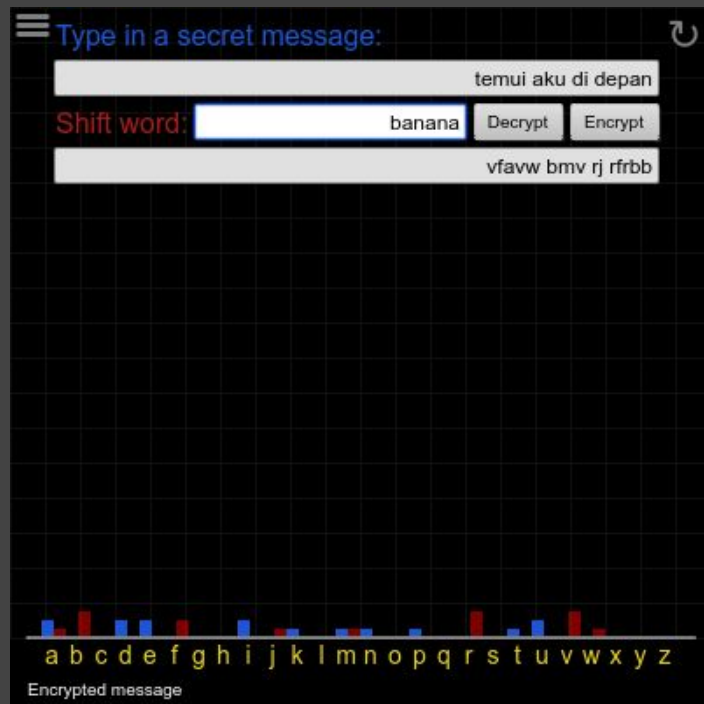
**Kelemahan dari caesar cipher telah dikemukakan oleh Al Kindi pada 800 SM, Yaitu dengan menggunakan analysis frequency huruf tergantung pada bahasa apa pesan itu ditulis.**

**Contoh Frequency Huruf =>**



# Polyalphabetic cipher

Mengingat Frequency Fingerprint merupakan kelemahan dari caesar cipher, maka solusinya adalah dengan menerapkan polyalphabetic cipher. Tidak berbeda jauh dengan cipher hanya saja jumlah pergeseran (shift) yang dilakukan tidak sama pada semua huruf tetapi sesuai dengan suatu kata kunci (shifter word).



	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

Vigenere cipher merupakan perluasan dari caesar cipher hanya saja menggunakann shift yang berbeda-beda

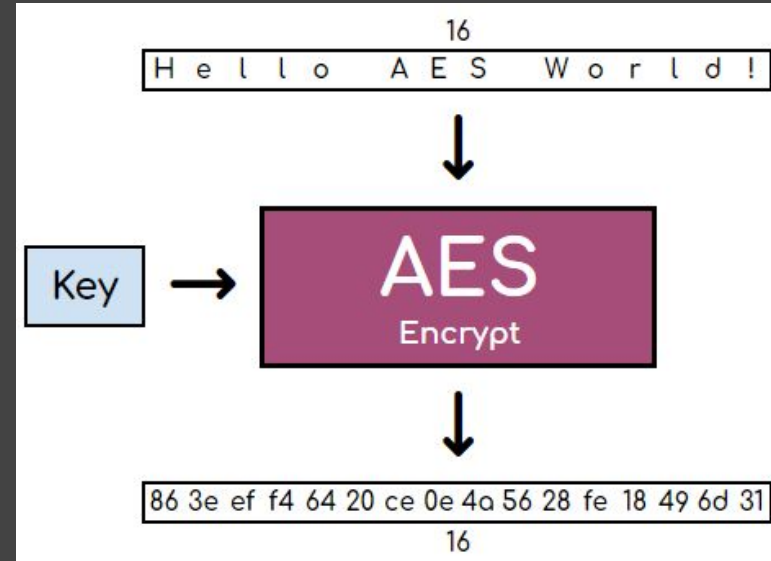
Table di samping ini bisa membantu untuk encoding teks.

Sebagai contoh, enkripsi kata CTFHAITIKUY dengan kunci **KODE**:

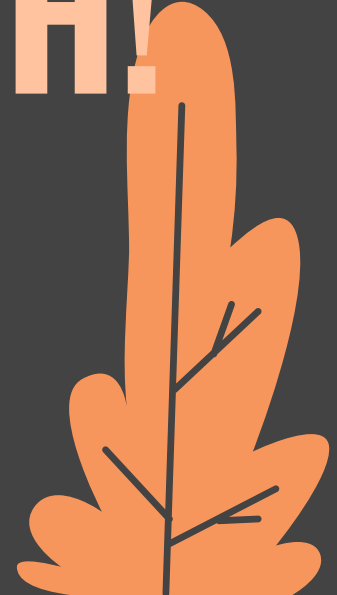
1. panjangkan **KODE** sepanjang kata yang mau di enkripsi, dalam kasus ini CTFHAITIKUY maka menjadi **KODEKODEKOD**
2. Untuk setiap huruf pada CTFHAITIKUY kita menggunakan table untuk mendapatkan huruf hasil enkripsi nya. Contoh untuk huruf pertama baris K dan kolom C
3. Huruf pertama chipertext nya adalah M
4. Jadi setelah semuanya, didapat **MHILKWWMUIB**


## AES (Advanced Encryption Standard)

Ada beberapa algoritma enkripsi yang sudah menjadi standar di negara tertentu, salah satunya adalah AES. Pada algoritma ini setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses. AES yang sering dipakai adalah AES-128, dimana artinya, kunci yang dipakai sepanjang 128 bit atau 16 byte.



**TAKE A BREATH!**





# STEGANO- GRAPHY

Seni menyembunyikan pesan dengan  
suatu cara

## Naon deui eta Steganography ?

Steganography adalah suatu teknik untuk menyembunyikan data.

Steganography sering dipakai di gambar dan audio.

Kita dapat mengirim gambar kucing dengan pesan di dalamnya, tanpa orang lain sadari bahwa ada pesan tersembunyi di gambar tersebut.



Viewable Message



**"Meet me at the  
park tonight at  
10pm"**

Hidden Message

## Naon deui eta Steganography ?

Tidak hanya sebuah pesan (tulisan), kita juga dapat menyisipkan suatu gambar ke gambar lainnya.



Viewable Message

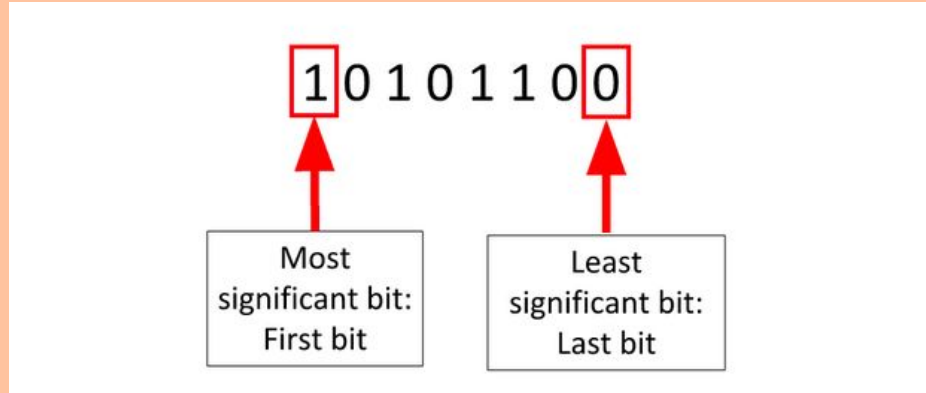


Hidden Message



# LSB Steganography

File terbuat dari banyak byte. Setiap byte terdiri dari 8 bit.



Mengganti LSB tidak akan terlalu berpengaruh

$$10101100_2 = 172_{10}$$

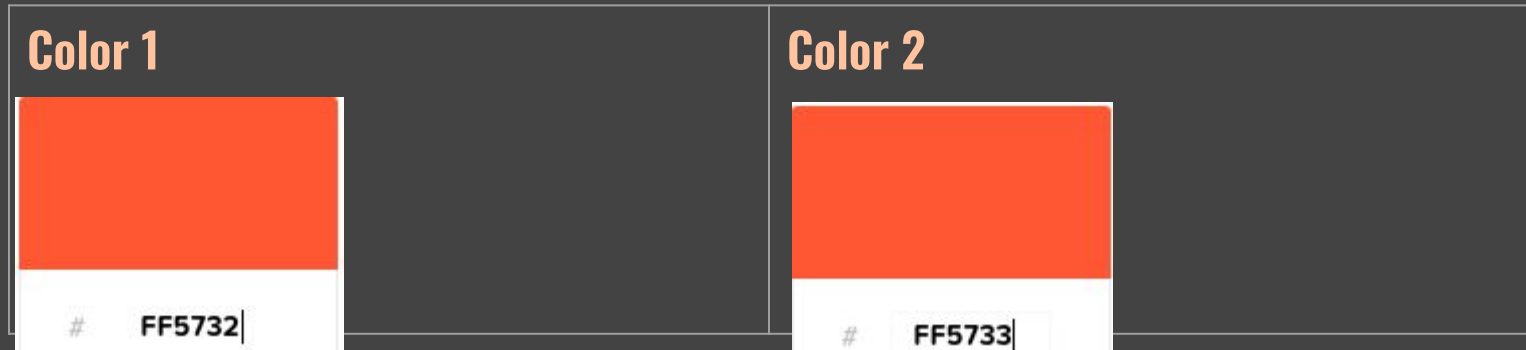
changing the LSB from '0' to '1':

$$10101101_2 = 173_{10}$$

Jadi kita bisa mengubah LSB tanpa diketahui bahwa suatu file tersebut sudah dimodifikasi. Jadi, kita bisa menyembunyikan sebuah pesan di sini.

Alasan sebuah steganography sukar untuk di deteksi karena perubahan hanya 1 bit tidak terlalu signifikan.

### Contoh:



Program stegsolve cukup generik untuk menyelesaikan berbagai bentuk steganografi dasar berdasarkan bit.

## **Metadata**

Penyembunyian data bisa dilakukan di metadata, jadi ketika kita memeriksa sebuah file secara menyeluruh, jangan lupa untuk memeriksa metadatanya terlebih dahulu.

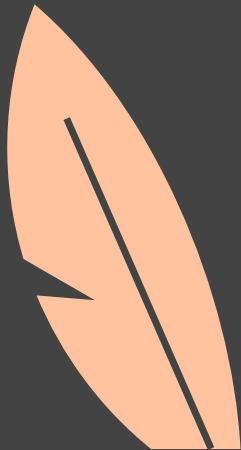
## **Image Editor**

Kuasailah penggunaan aplikasi image editor (seperti GIMP, atau Photoshop) karena sebagian soal mudah dapat diselesaikan dengan cara ini.

## **Audio**

Analysis signal audio dapat dilakukan dengan audacity. Selain Memiliki waveform view, audacity juga memiliki spectogram view.

# EXERCISE



1. 333 555 2 4 66 999 2 0 2 3 2 555 2 44 0 44 2 444 8 444 { 3 666 66  
8 333 666 777 4 33 8 55 33 999 7 2 3 } 7777 33 22 33 555 88 6 0 6  
88 66 222 88 555 0 77 9 33 777 8 999

2. 000 0 0100 01 11 01 1 101 0 0110 01 100 01 01 10 100 01 1011 01  
10 110 11 01 000 00 0000 1 0 010 001 000 1000 0 010 1 01 0000  
01 10 100 00 1010 1 0010 0000 01 00 1 00 00 10 00 110011 11  
01 101 01 100 01 010 00 00 1 001 00 10 00 0010 0100 01 110  
10 1011 01 0000 01 00 1 00 { 000 01 11 001 0 0100 11 111 010 000 0  
}

3. Mari petak umpet dengan si lucu ini

<https://drive.google.com/file/d/1Tmuw-ynEqj1R8bKDWA8KHuts9CdVaTPy/view?usp=sharing>

4. Jangan lupa LSB ya.

[https://drive.google.com/file/d/13lazaMB\\_A7miokGqTI52rlpn0eXQVvHc/view?usp=sharing](https://drive.google.com/file/d/13lazaMB_A7miokGqTI52rlpn0eXQVvHc/view?usp=sharing)

5. haiti adalah kunci segalanya

cioxvlrm bbb sigoht abuwet, riug zbjlt bnp tevviyi sxg uyi. bvp dqt  
nsaoggh yi aiptq{vzfpbh\_qz\_eilg}, wettrhrq vqwhmk ghno eipnvri.

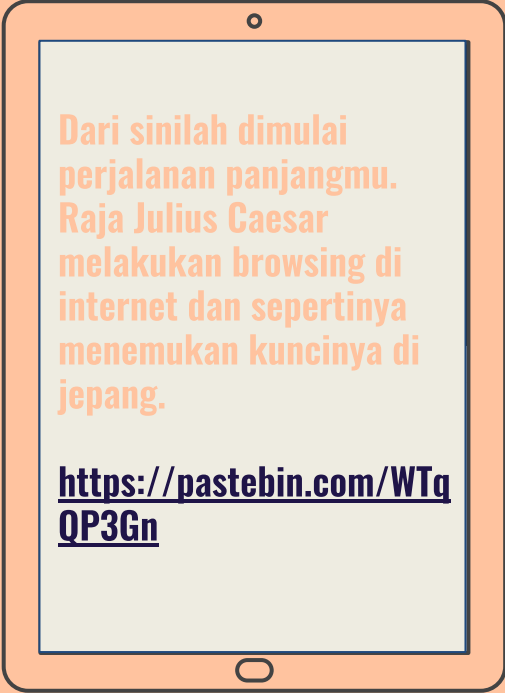
6. GAS... (Gunakan Algoritma Standar)

kuncinya = haiti

usJwaSzEOqJb99lyrBdLu1dq+iVfU2KGn72zGOzXx/kSNORQ5hm+I/NGA8  
+4A4IL

# CHALLENGE





Dari sinilah dimulai  
perjalanan panjangmu.  
Raja Julius Caesar  
melakukan browsing di  
internet dan sepertinya  
menemukan kuncinya di  
jepang.

<https://pastebin.com/WTgQP3Gn>

1



Seseorang bisa menyembunyikan sesuatu, begitu pula dengan sebuah gambar.  
Setidaknya perjalanan disini lebih singkat dari perjalanan sebelumnya.

<https://drive.google.com/file/d/198uFyl50P182SOJSZWfkCzq3kdjiFR4x/view?usp=sharing>

2

# OUR TEAM

**CIPTO TRI UTOMO**

Teknik Informatika 2015

**ASEP BUDIYANA  
MUHARAM**

Teknik Informatika 2018





# NUHUNS!

Kalo ada pertanyaan bisa dicoba komentar di  
google classroom atau melalui official Account Abit

Credit::

- ◀ [ctf101.org](https://ctf101.org)
- ◀ <https://yohan.es>
- ◀ <https://picoctf.com>