CRYPTOGRAPHY AND STEGANOGRAPHY

Department of Informatics

Session 1 – Introduction to Cryptography

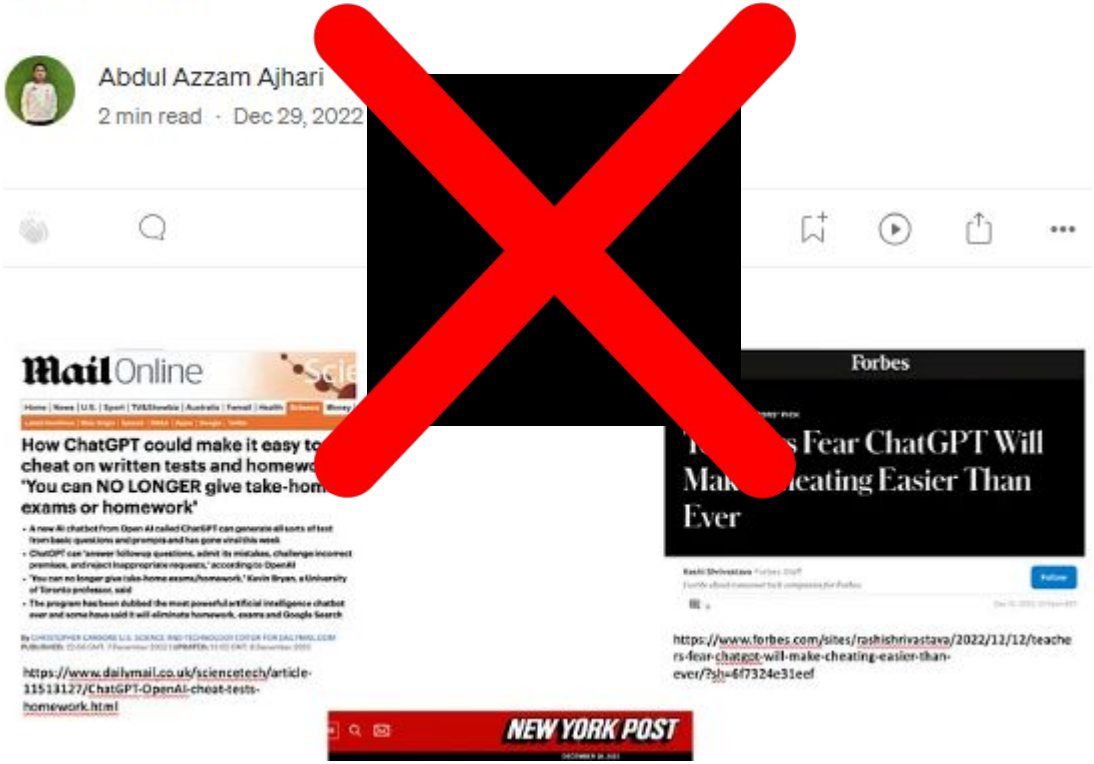
Ambros Magnus Rudolf Mekeng, S.T.,M.T

Abdul Azzam Ajhari, S.Kom., M.Kom.

Study Contract

- UTS (Week 8) 30%
- UAS (Week 16) 30%
- Task 1 & Task 2 (Personal/Group) 30%
- Attendance, Quizzes, Attitude & Behavior 10%

Preventing Student Cheating in Indonesia using OpenAI Based on RoBERTa OpenAI Detector (GPT-2 Model)



Cheating

=

AUTO NULL

Who is Azzam?

https://linktr.ee/abdulazzamajhari

BSSN
2019 - current
Informatics Expert

Binus Graduate Program
2020 - 2022
S-2 (MCs) Computer Science
Data Scientist

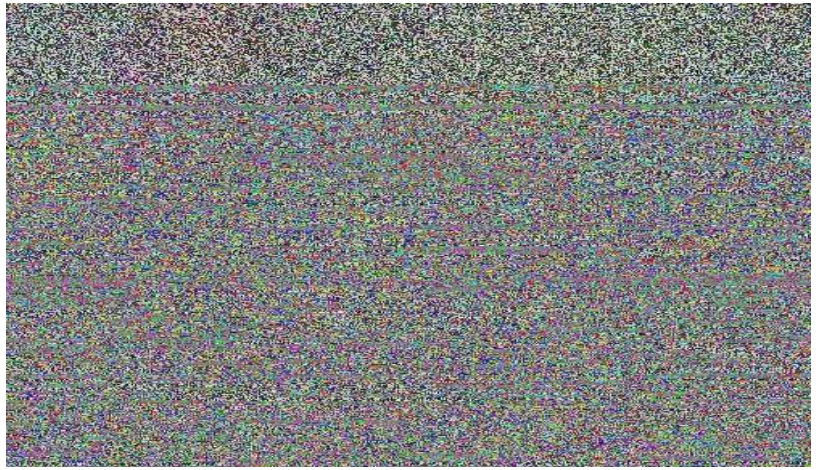
Garudafood Group
2018 - 2019
IT System Development Officer

Universitas Budi Luhur
2014 - 2018
S-1 (BCs) Computer Science
Cybersecurity

Can you understand the following information?

Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/ p}âpx;
épêp/|t}t|äzp}/qp}êpz/étzp{x/zt xâx
}v êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p psp{pw/p}pz<p}pz/zt xâx}v/êp}
v/qpüä |t}tâpé/spüx/sp{p|/ péxü=/]
p{äüx |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw ât| pâ/ztwxsä p}/|tützp=

(1)



(2)

If you can't read it, here is the original information:

Ketika saya berjalan-jalan di pantai, saya menemukan banyak sekali kepiting yang merangkak menuju laut. Mereka adalah anak-anak kepiting yang baru menetas dari dalam pasir. Naluri mereka mengatakan bahwa laut adalah tempat kehidupan mereka.

(1)

(2)

- Information that cannot be understood is called ciphertext.
- On the other hand, information that can be understood is called plaintext.
- Plaintext can be transformed into ciphertext, and vice versa.
- The transformation of plaintext into ciphertext is done using cryptography.

- The word cryptography comes from Greek :

  κρυπτο (*hidden* or *secret*) and γραφη (*writing*)

  Its mean "*secret writing*"

  Cryptography is the science and art of maintaining the confidentiality of messages by encoding them into a form that cannot be understood.

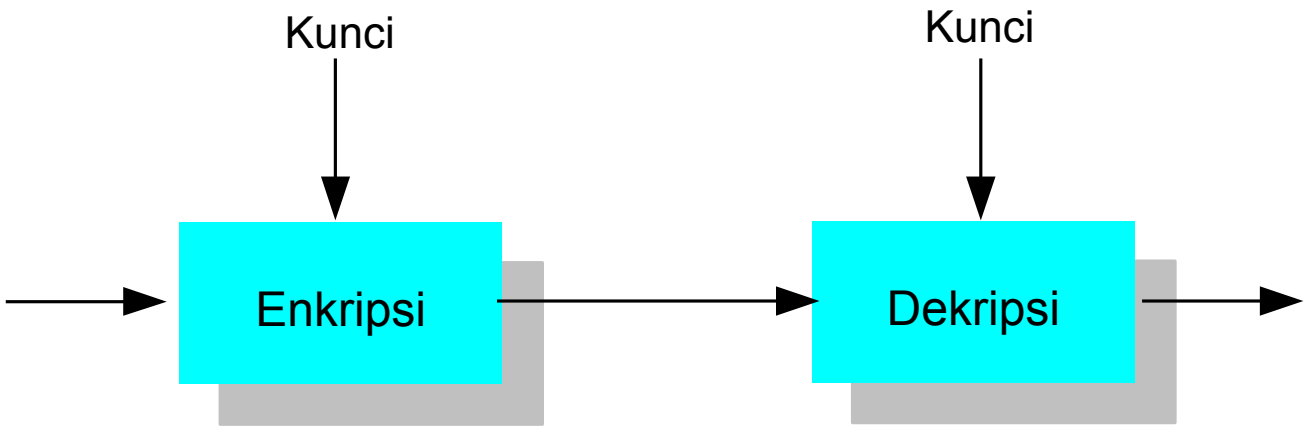
- Cryptography terms in Indonesian:

  Science of Cryptography / Ilmu Persandian

Cryptography consists of two processes:

1. Encryption: transformation from plaintext to ciphertext
2. Decryption: transformation from ciphertext to plaintext

Both use secret keys

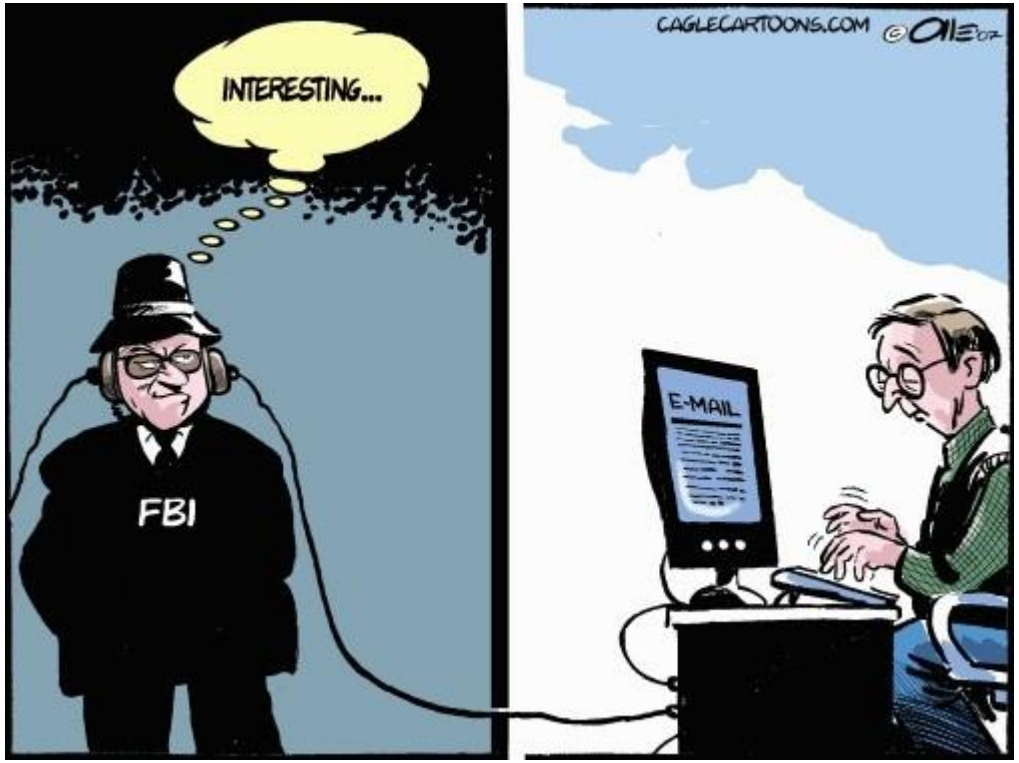


- Why is cryptography so important today? to maintain the confidentiality of information
  - state confidential data/information
  - organization confidential data/information
  - personal data/information

- In today's digital era, the exchange of information is vulnerable to third-party eavesdropping.

- Cryptography is useful for securing confidential information so that it does not leak to the public.

Tapping



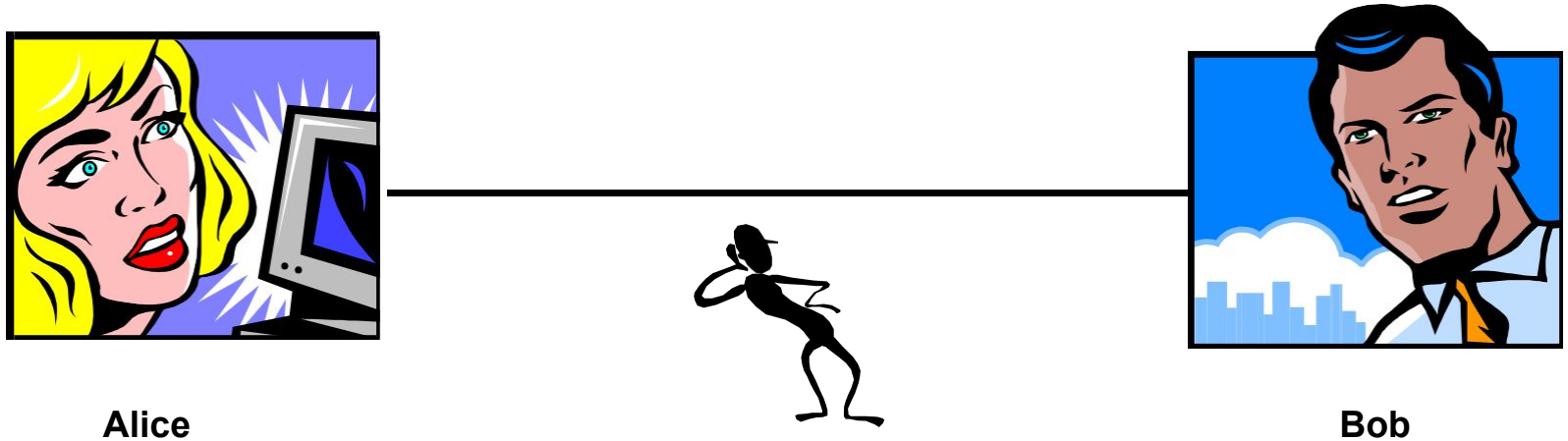
1. Wiretapping

15506-41DG
'Office: 9am' Disc
© JupiterImages

Creatas
www.comstock.com

2. Acoustic Eavesdropping

3. Electromagnetic eavesdropping



With the science and technology of cryptography, information is presented in the form of ciphertext so that third parties cannot understand its meaning.

Data Encryption on Motion

- Signals transmitted in a conversation with a mobile phone.
- ATM card PIN numbers transmitted from an ATM machine to a bank computer.
- Credit card PIN numbers in e-commerce transactions on the internet.
- Pay TV broadcasts
- Messages via BlackBerry Messenger (BBM), WhatsApp, Telegram, etc

Cryptographic Elements

1. Cryptographic algorithm (cipher)

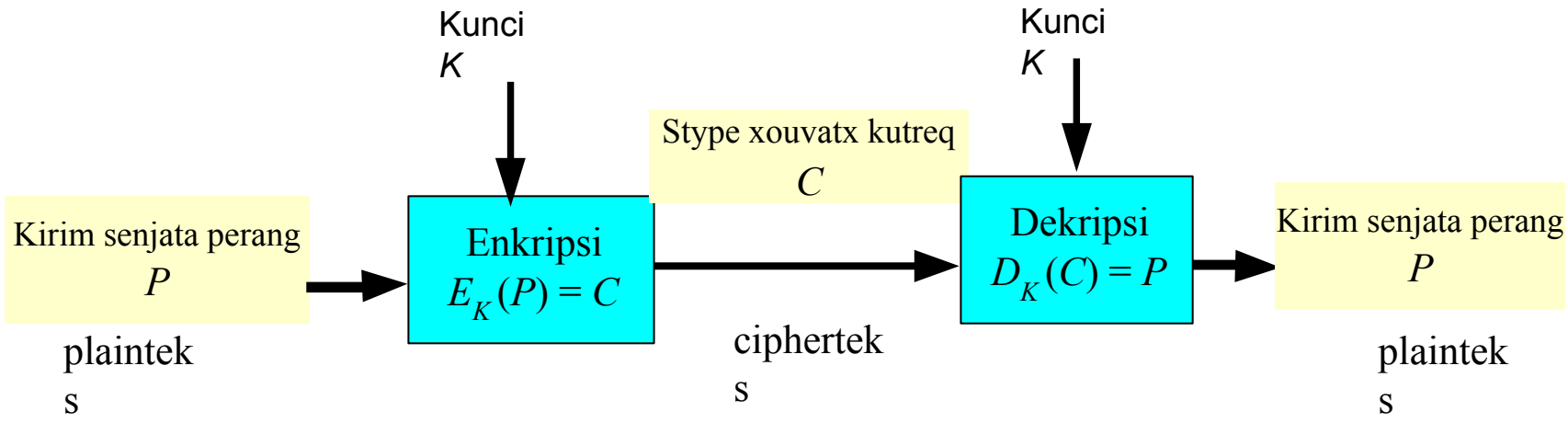
   Rules for encryption and decryption, or mathematical functions used for encryption and decryption.

2. Key

   Parameters used for encryption and decryption transformations. Keys are secret, while cryptographic algorithms are not secret (public)

3. Message

   Information that is encrypted/decrypted


Kunci
K
Kunci
K
Stype xouvatx kutreq
C
Kirim senjata perang
P
Enkripsi
$E_K(P) = C$
Dekripsi
$D_K(C) = P$
Kirim senjata perang
P
plaintek
s
ciphertek
s
plaintek
s

Cryptography does not solve privacy problems, but it is a useful tool

THANK YOU