
CRYPTOGRAPHY


IN OUR CLASSROOM
WE RESPECT EACH OTHER.
WE TRY OUR BEST.
WE ARE A TEAM.
WE LEARN FROM MISTAKES.
WE CREATE.
WE CELEBRATE EACH OTHER'S SUCCESS.
TEACHFACTORY.COM

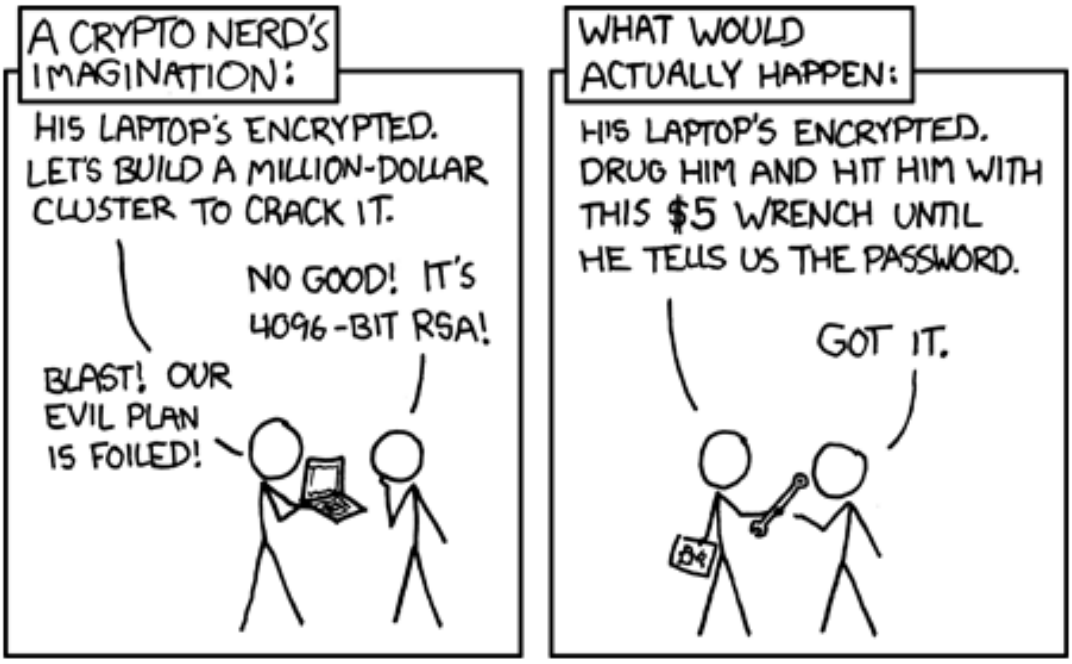
SERANGAN PADA CRYPTOGRAPHY

CAPAIAN PEMBELAJARAN

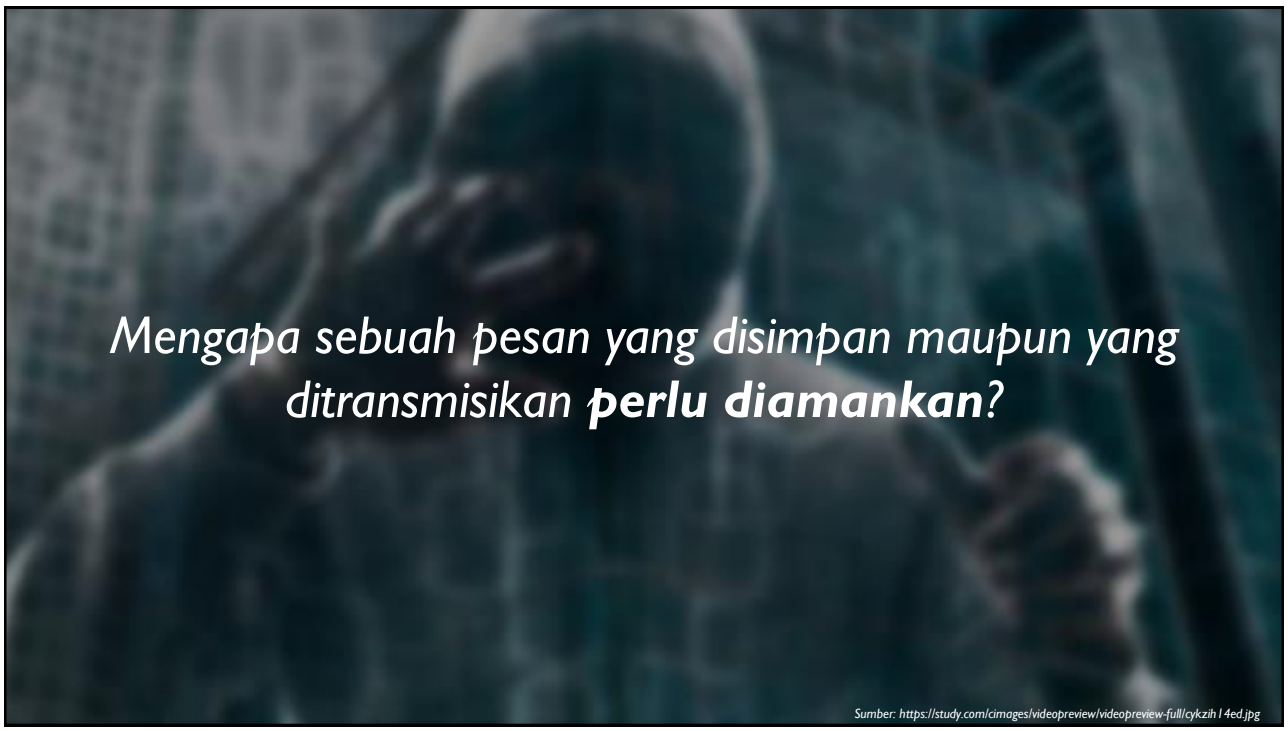
- Mahasiswa memahami konsep serangan terhadap kriptografi
- Mahasiswa memahami jenis-jenis serangan terhadap kriptografi
- Mahasiswa memahami teknik serangan terhadap kriptografi

Agenda.

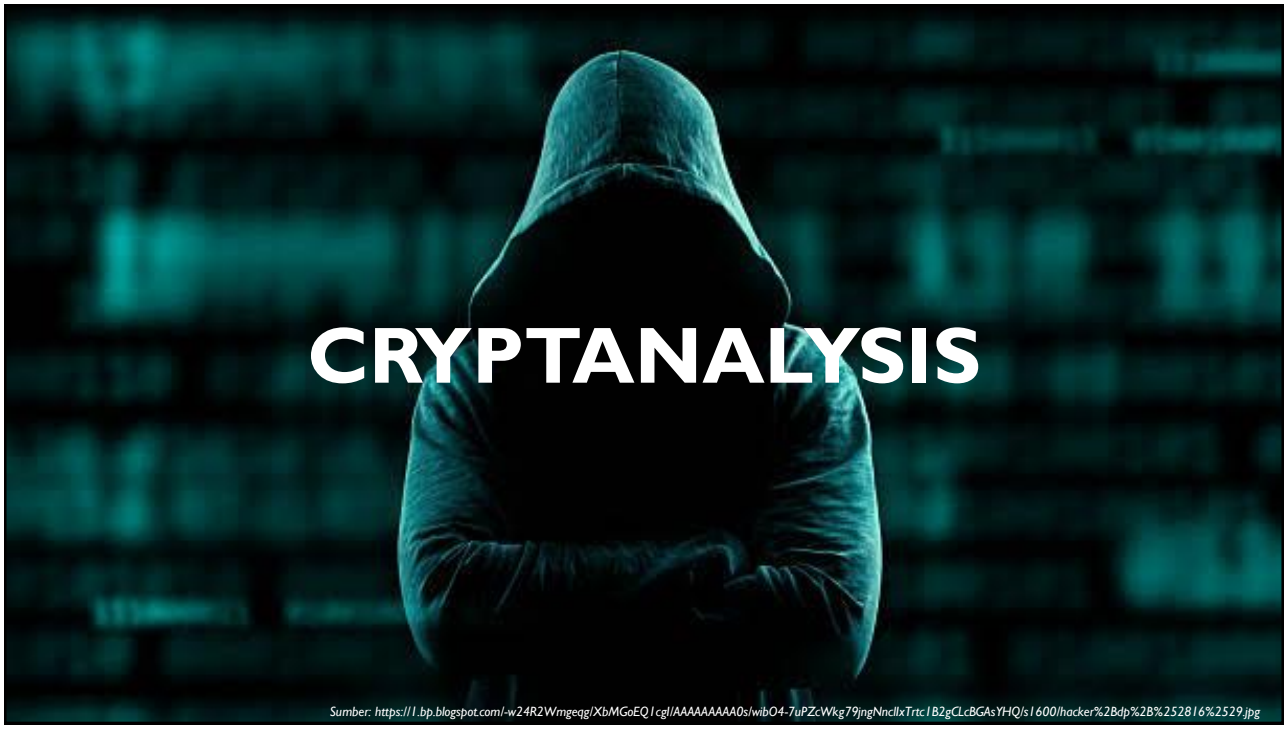
- Cryptanalysis
- Klasifikasi cryptanalysis attack
  - Jenis informasi
  - Teknik serangan
- Jenis serangan



Sumber: https://static.wixstatic.com/media/6a4a49_3d364bbbad1f46e488bfa10aac8b461f~mv2.png/v1/fit/w_300,h_300,al_c,q_5/file.png



Sumber: https://study.com/cimages/videopreview/videopreview-full/cykzih14ed.jpg



Sumber: https://1.bp.blogspot.com/-w24R2Wmgeqg/XbMGoEQ1cgI/AAAAAAAAA0s/wibO4-7uPZcWkg79jngNncIlxTrtc1B2gCLcBGAsYHQ/s1600/hacker%2Bdp%2B%252816%2529.jpg

CRYPTANALYSIS

- Penyadap yang melakukan serangan untuk mendapatkan sebanyak-banyaknya data yang digunakan untuk melakukan kriptografi
- Individu yang bertujuan untuk memecahkan ***chiperteks*** menjadi ***plainteks*** tanpa memliliki akses ke kunci yang digunakan disebut dengan ***cryptanalysis***.
- Kriptanalisis menggunakan segala cara untuk mendapatkan sebanyak-banyaknya data untuk dapat mengetahui isi pesan yang terenkripsi.

8

CRYPTANALYSIS ATTACK

- **Cryptanalysis attack:** serangan yang menggunakan informasi yang tersedia untuk melakukan kriptanalisis dengan tujuan menemkan kunci atau plainteks.
- **Cryptanalysis attack** dapat diklasifikasikan menjadi 2 kelompok
  1. Berdasarkan jenis informasi yang tersedia
  2. Berdasarkan teknik serangan

9

CRYPTANALYSIS ATTACK | JENIS INFORMASI

Chipertext-only Attack.

- Kriptanalisis hanya menggunakan informasi chiperteks yang tersedia saja.
- Kriptanalsis hanya mengetahui algoritma enkripsi yang digunakan dalam mentransformasikan plainteks menjadi chiperteks.
- Tugasnya adalah menemukan plainteks sebanyak mungkin dari chiperteks tersebut.
- Kriptanalisis menggunakan segala cara (*brute-force*) dan mencoba menerka plainteks berdasarkan informasi yang ada.

10

CRYPTANALYSIS ATTACK | JENIS INFORMASI

Known-plaintext Attack.

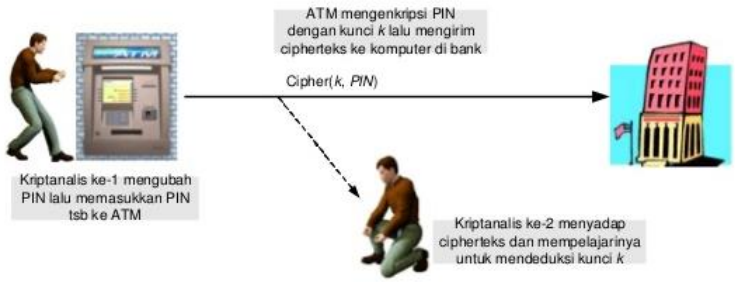
- Kriptanalisis melakukan serangan dengan menggunakan informasi beberapa pasangan plainteks dan chiperteks yang tersedia saja.
- Plainteks mungkin diperoleh dengan mempelajari karkateristik pesan
- Contoh dari plainteks yang mudah diterka adalah pesan yang dituliskan secara formal atau email yang menggunakan kata "*From*" atau "*To*"

11

CRYPTANALYSIS ATTACK | JENIS INFORMASI

Chosen-plaintext Attack.

- Kriptanalisis memiliki kemampuan dalam memilih plainteks yang dimilikinya yang diasumsikan lebih mengarah ke penemuan *key*.



12

Sumber: https://image.slidesharecdn.com/01seranganterhadapkriptografi2013-140807225413-phpapp01/95/kriptografi-serangan-terhadap-kriptografi-28-638.jpg?cb=1412566922

CRYPTANALYSIS ATTACK | JENIS INFORMASI

Adaptive-chosen-plaintext Attack.

Kriptanalisis memilih blok plainteks yang besar, lalu dienkripsi, kemudian kriptanalisis memilih blok plainteks yang lebih kecil berdasarkan serangan sebelumnya, begitu seterunya.

Chosen-chipertext Attack.

Kriptanalisis memilih chiperteks untuk didekripsikan dan memilih akses ke plainteks hasil dekripsi otomatis.

13

CRYPTANALYSIS ATTACK | JENIS INFORMASI

Chosen-text Attack.

Merupakan serangan kriptanalisis yang menkombinasikan antara *chosen-plaintext attack* dan *chosen-chipertext attack*.

14

CRYPTANALYSIS ATTACK | TEKNIK SERANGAN

Brute-force Attack.

- Serangan untuk menemukan kunci dengan mencoba semua kemungkinan kunci.
- Semakin panjang kunci, maka jumlah kemungkinan diterka semakin besar.

Analytic Attack.

- Kriptanalisis tidak akan mencoba-coba semua kemungkinan kunci, tetapi melakukan analisis kelemahan algoritma kriptografi untuk mengurangi kemunkinan kunci yang tidka ada.

15

JENIS SERANGAN CRYPTANALYSIS

- Terdapat 2 jenis serangan kriptanalisis yang tidak secara langsung menyerang sistem kriptografi
- Jenis serangan ini lebih kepada untuk mendapatkan sebanyak mungkin informasi penting yang kan digunakan untuk memecahkan sistem kriptografi.
- Jenis serangan ini berhubungan dengan ada atau tidaknya keterlibatan penyerang di dalam komunikasi.
- Jenis serangan tersebut adalah; (1) ***passive attack*** dan (2) ***active attack***

16

JENIS SERANGAN CRYPTANALYSIS

Passive Attack.

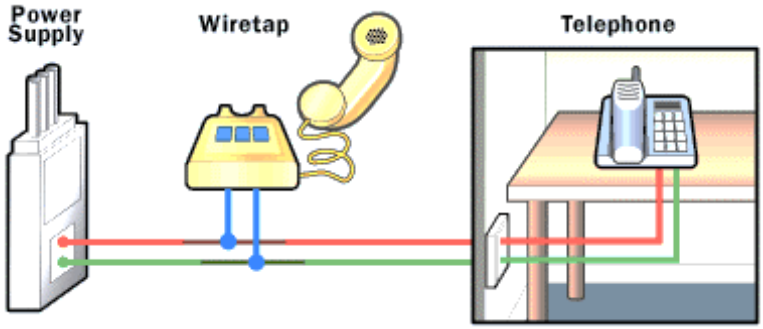
- Penyerang tidak turut terlibat dalam komunikasi antara pengirim dan penerima.
- Penyerang menyadap semua pertukaran pesan antara pengirim dan penerima dengan tujuan untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis.
- Metode penyadap data.
  - ***Wiretapping***;
  - ***Electromanetic eavesdropping***;
  - ***Accoustic eavesdropping***.

17

JENIS SERANGAN CRYPTANALYSIS

Wiretapping.

Penyadap mencegat data yang ditransmisikan melalui saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.



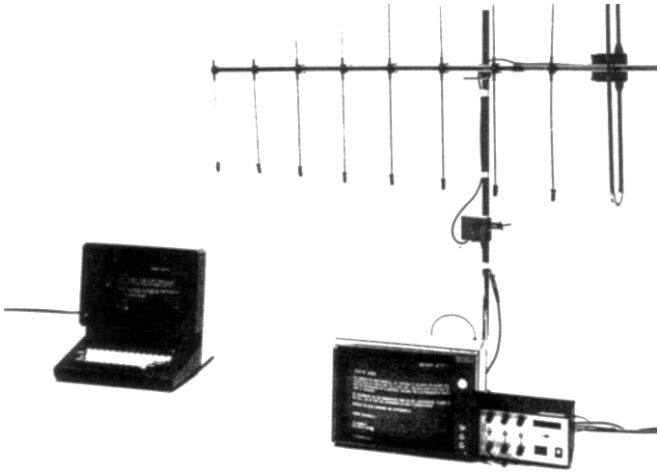
Sumber: https://hackaday.com/wp-content/uploads/2008/06/had-wiretap.jpg

18

JENIS SERANGAN CRYPTANALYSIS

Electromagnetic Eavesdrop.

Penyadap mencegat data yang ditransmisikan melalui saluran *wireless*.



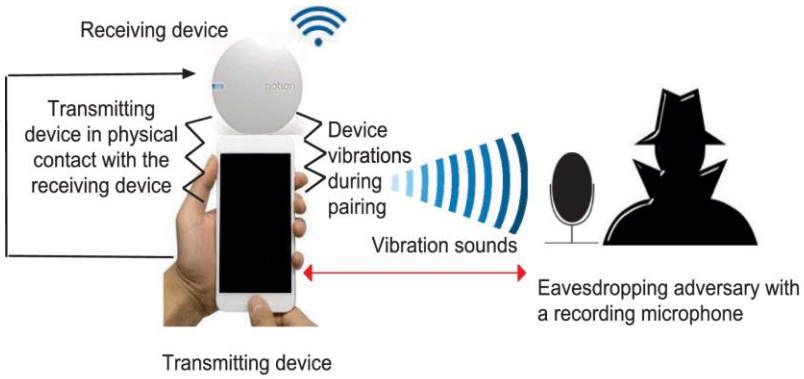
Sumber: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRQm8RXt-5k-dLGsviLRZAYkKnzTbPriH4OK0D0L5CjXIW8K-ILeA&s

19

JENIS SERANGAN CRYPTANALYSIS

Accoustic Eavesdrop.

Penyadap mencegat data dalam gelombang suara yang dihasilkan oleh manusia.



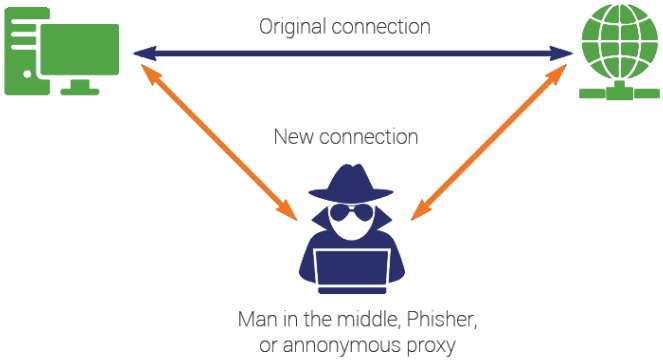
Sumber: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRQm8RXt-5k-dLGsviLRZAYkKnzTbPriH4OK0D0L5CjXIW8K-ILeA&s

20

JENIS SERANGAN CRYPTANALYSIS

Active Attack.

Penyerang melakukan intervensi komunikasi dan turut mempengaruhi sistem untuk keuntungan dirinya dengan cara mengubah aliran pesan agar dapat memodifikasi chiperteks.



Sumber: https://www.thesslstore.com/blog/wp-content/uploads/2018/11/man-in-the-middle-attack.png

21

SERANGAN PADA CRYPTOGRAPHY