Serangan Terhadap Kriptografi

Pendahuluan

- Keseluruhan *point* dari kriptografi adalah menjaga kerahasiaan pesan atau kunci dari penyadap (*eavesdropper*) atau dari kriptanalis (*cryptanalyst*).

- Kriptanalis dapat merangkap sebagai seorang penyadap

- Kriptanalis berusaha memecahkan cipherteks dengan suatu serangan terhadap sistem kriptografi.

Serangan (*attack*)

- **Serangan**: setiap usaha (*attempt*) atau percobaan yang dilakukan oleh kriptanalis untuk menemukan kunci atau menemukan plainteks dari cipherteksnya.
- Asumsi: kriptanalis mengetahui algoritma kriptografi yang digunakan

Prinsip Kerckhoff: Semua algoritma kriptografi harus publik; hanya kunci yang rahasia.

Satu-satunya keamanan terletak pada kunci!

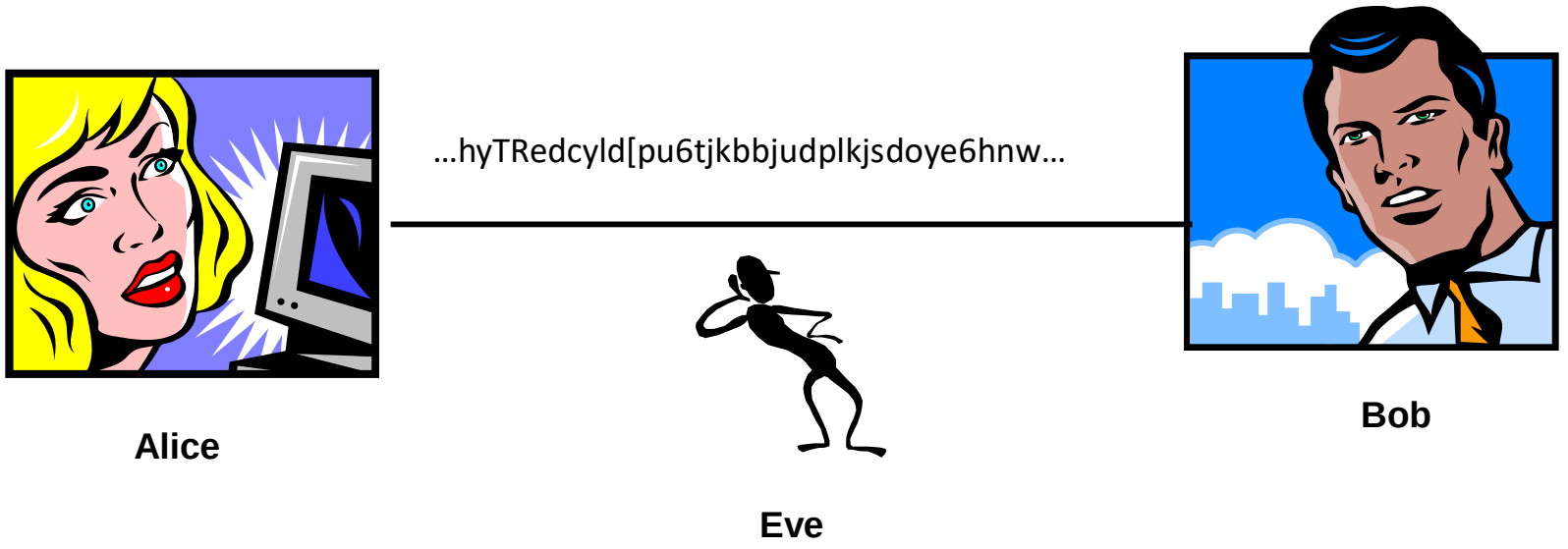
Jenis-jenis Serangan

Berdasarkan keterlibatan penyerang dalam komunikasi**:**

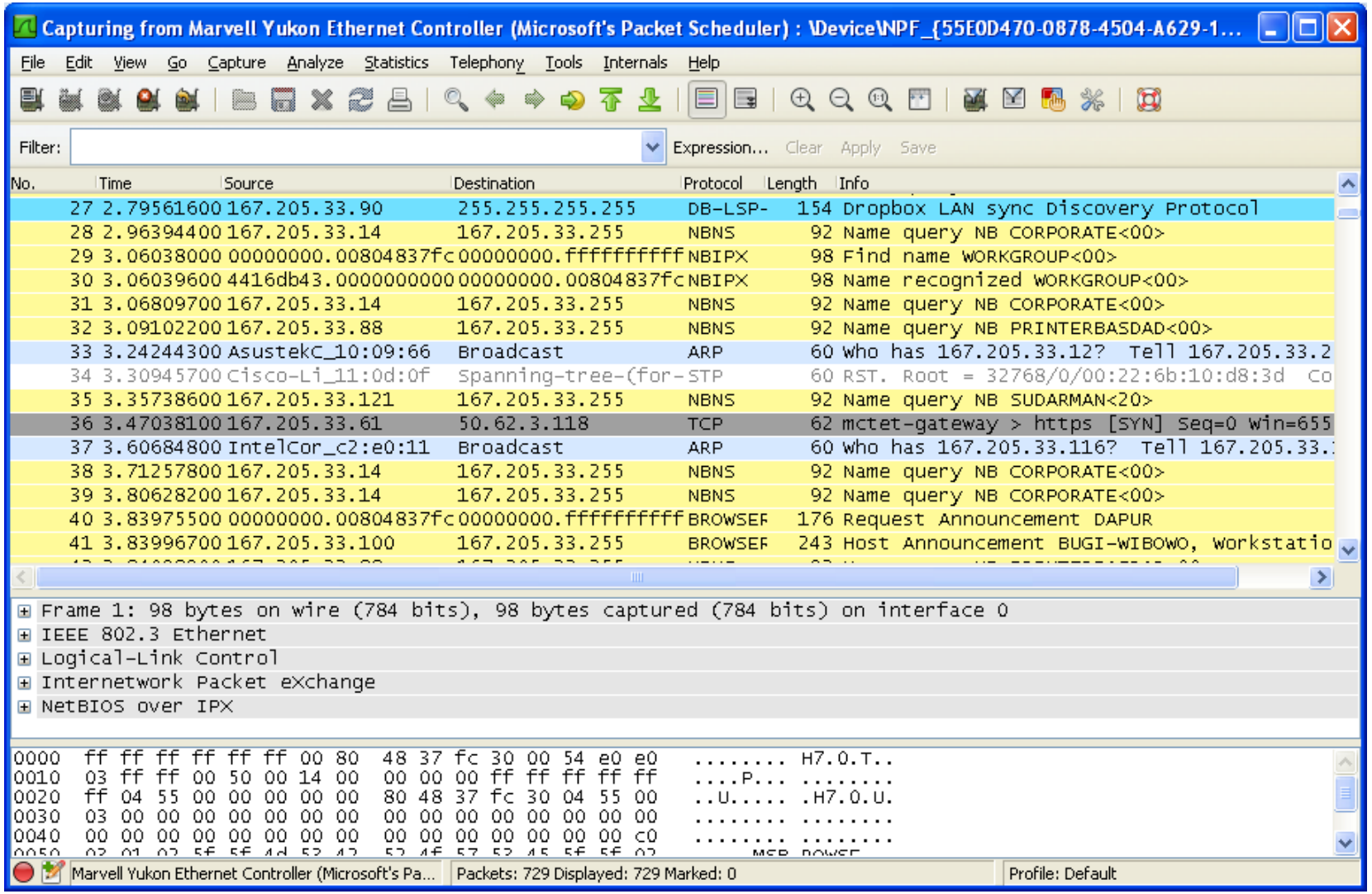
1. **Serangan pasif**
2. **Serangan aktif**

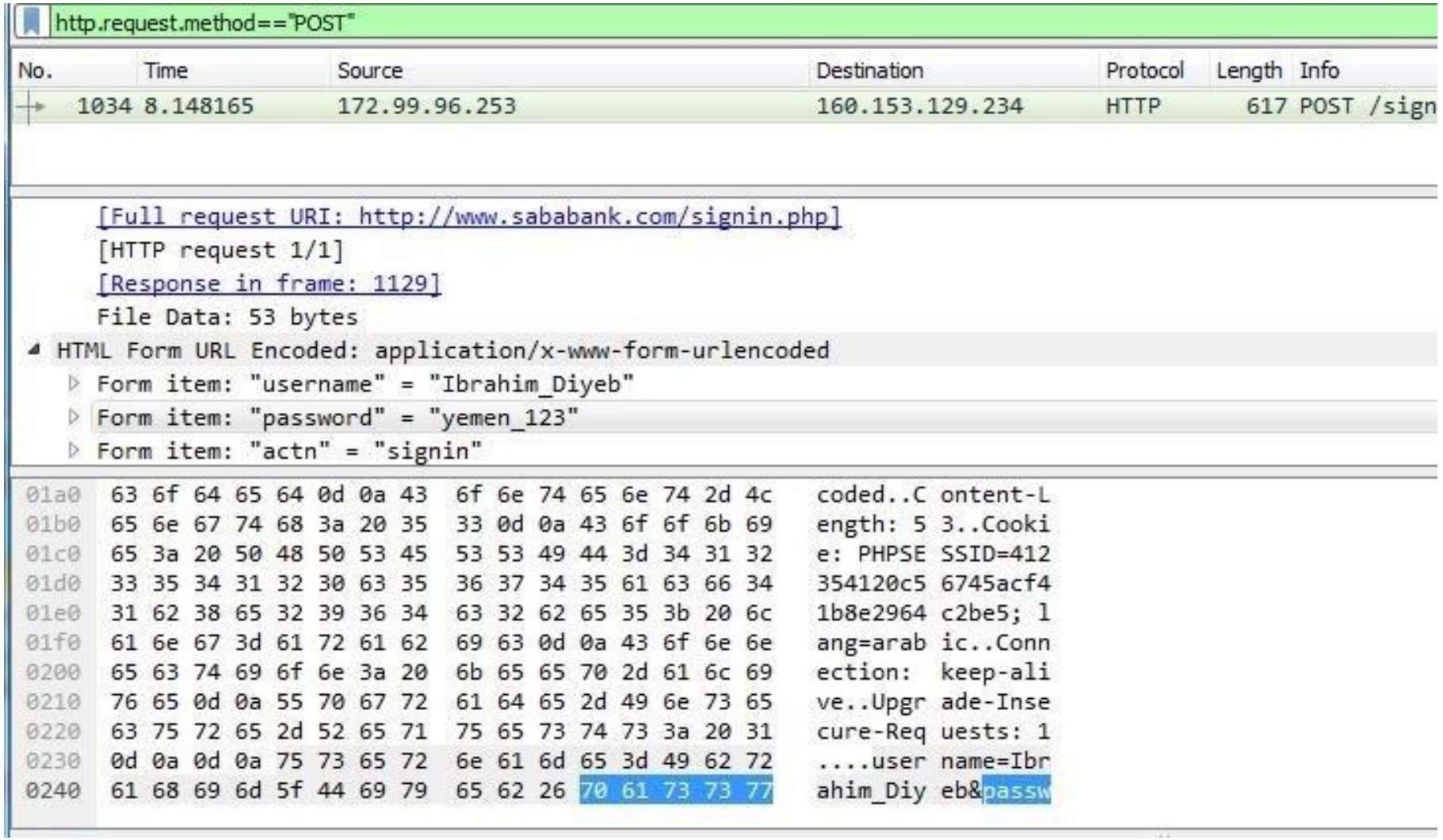
1. Serangan pasif (*passive attack*)

- penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima
- penyerang hanya melakukan penyadapan untuk memperoleh data atau informasi sebanyak-banyaknya



Screenshot Wireshark (memantau *network traffic*)





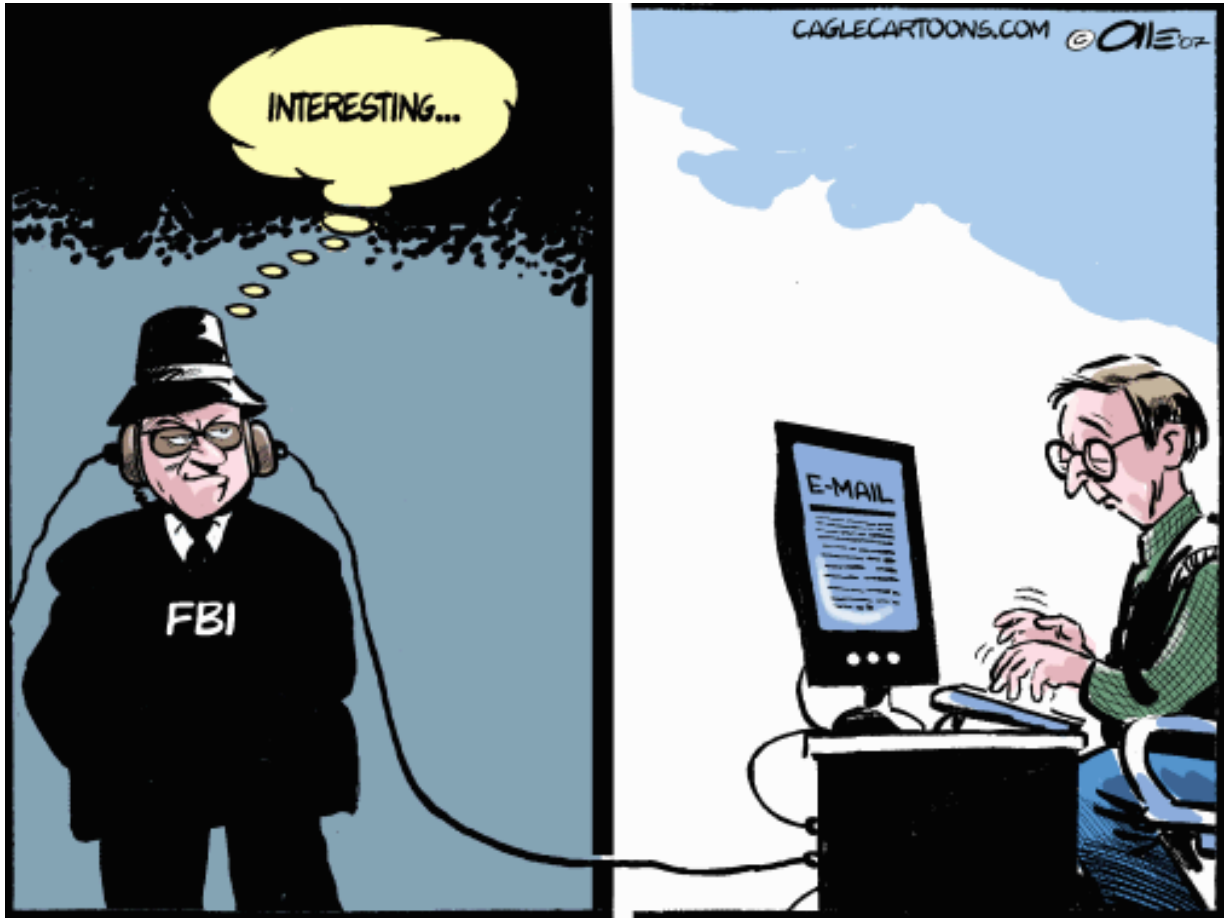
Filtering dengan Wireshark dapat menampilkan plainteks berupa *username* dan *password*

Sumber gambar: https://www.researchgate.net/figure/Wireshark-Filtering-Showing-Clear-Text-of-user-Name-and-Password_fig3_326419957

Metode penyadapan:

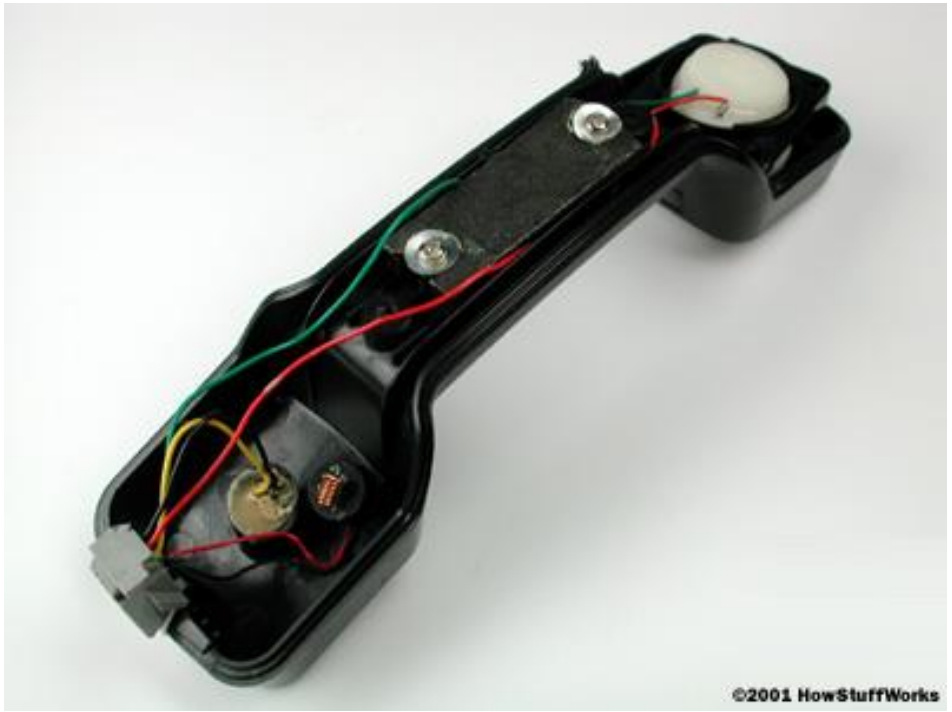
1. *Wiretapping*
2. *Electromagnetic eavesdropping*
3. *Acoustic Eavesdropping*

- *Wiretapping*



How Wiretapping Works

(sumber: http://www.howstuffworks.com/wiretapping.htm)



When you open up a phone, you can see that the technology inside is very simple. The simplicity of design makes the phone system vulnerable to surreptitious eavesdropping.

Inside a standard phone cord, you'll find a red wire and a green wire. These wires form a circuit like the one you might find in a flashlight. Just as in a flashlight, there is a negatively-charged end and a positively-charged end to the circuit. In a telephone cord, the green wire connects to the positive end and the red cord connects to the negative end.

Electromagnetic eavesdropping

Lihat info alat penyadap suara GSM:

http://indonetwork.web.id/Matama_Security/1168831/spy-ear-gsm-penyadap-suara-dengan-kartu-gsm.htm

Acoustic Eavesdropping

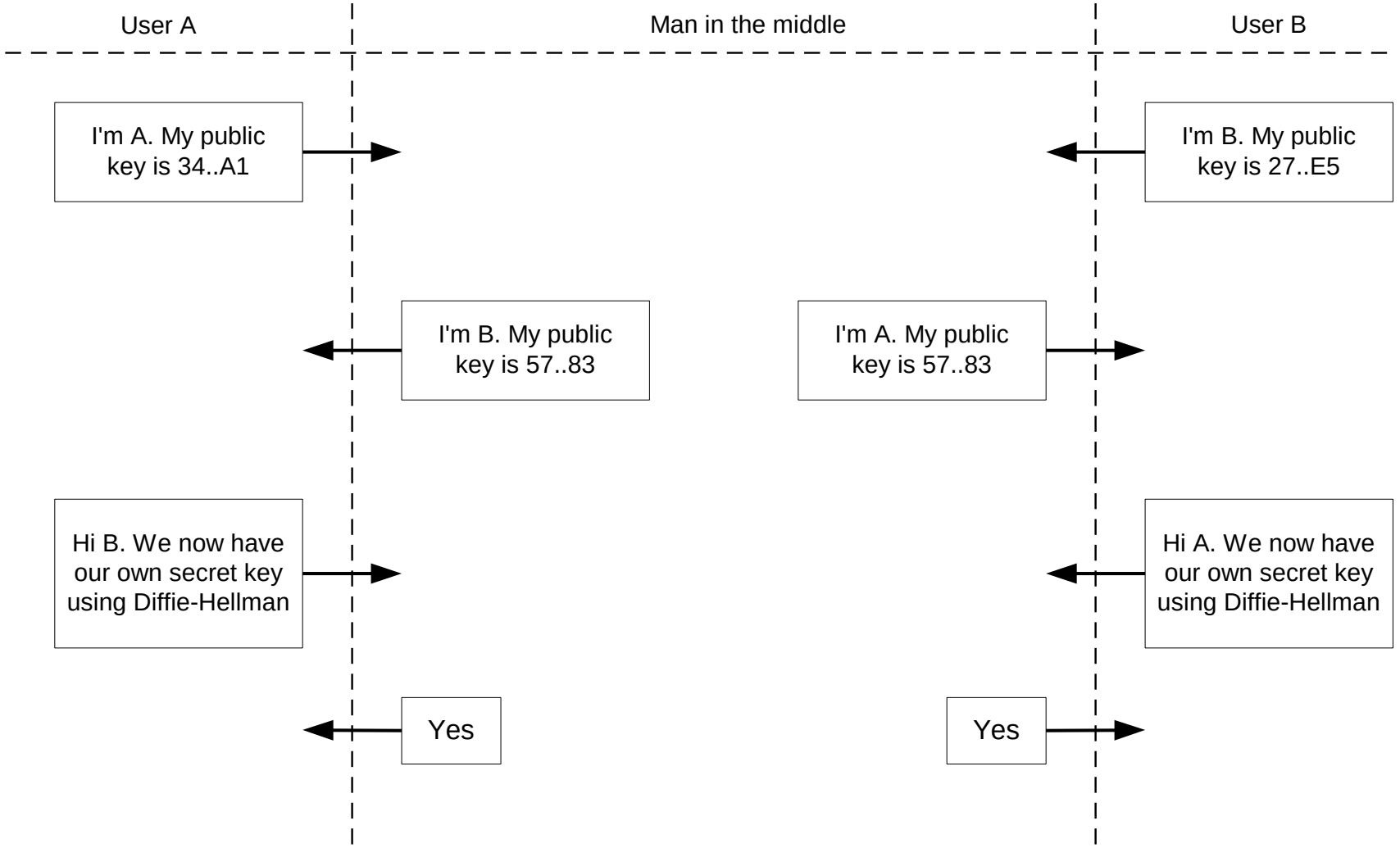
2. Serangan aktif (*active attack*)

- penyerang mengintervensi komunikasi dan ikut mempengaruhi system untuk keuntungan dirinya

- penyerang mengubah aliran pesan seperti:
  - menghapus sebagian cipherteks,
  - mengubah cipherteks,
  - menyisipkan potongan cipherteks palsu,
  - me-*replay* pesan lama,
  - mengubah informasi yang tersimpan, dsb

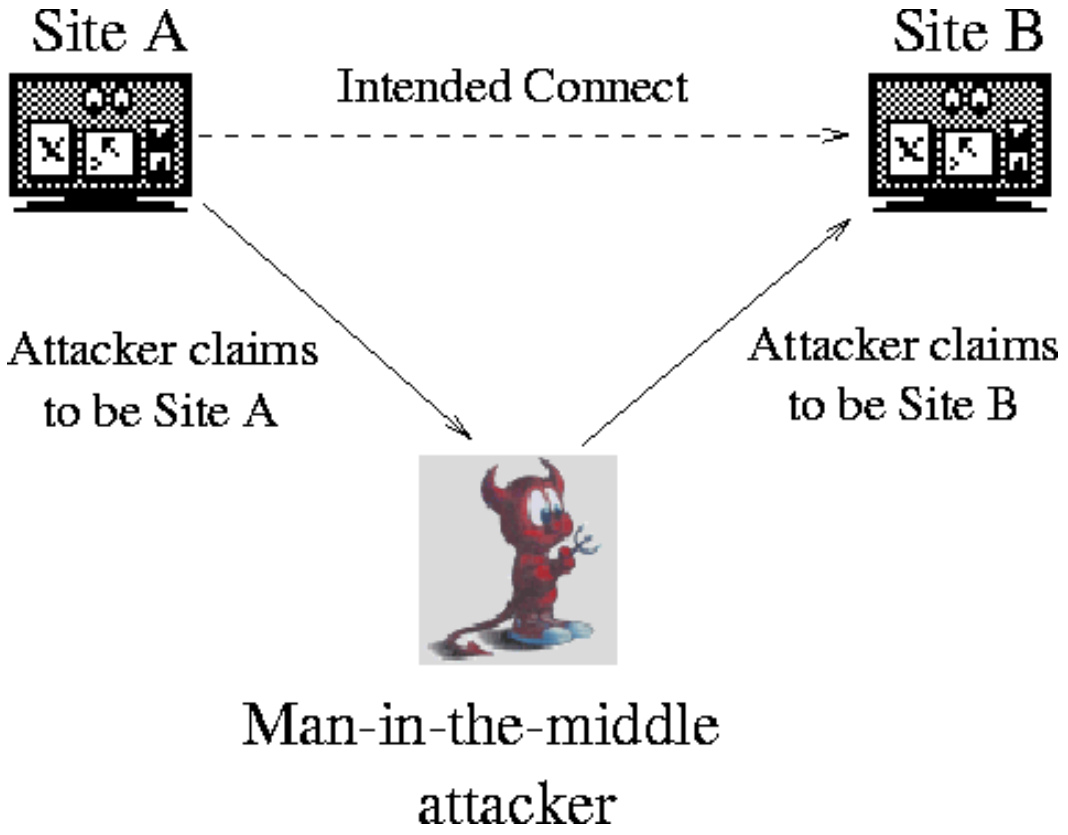
- Contoh: *man-in-the-middle attack*

Man-in-the-middle-attack

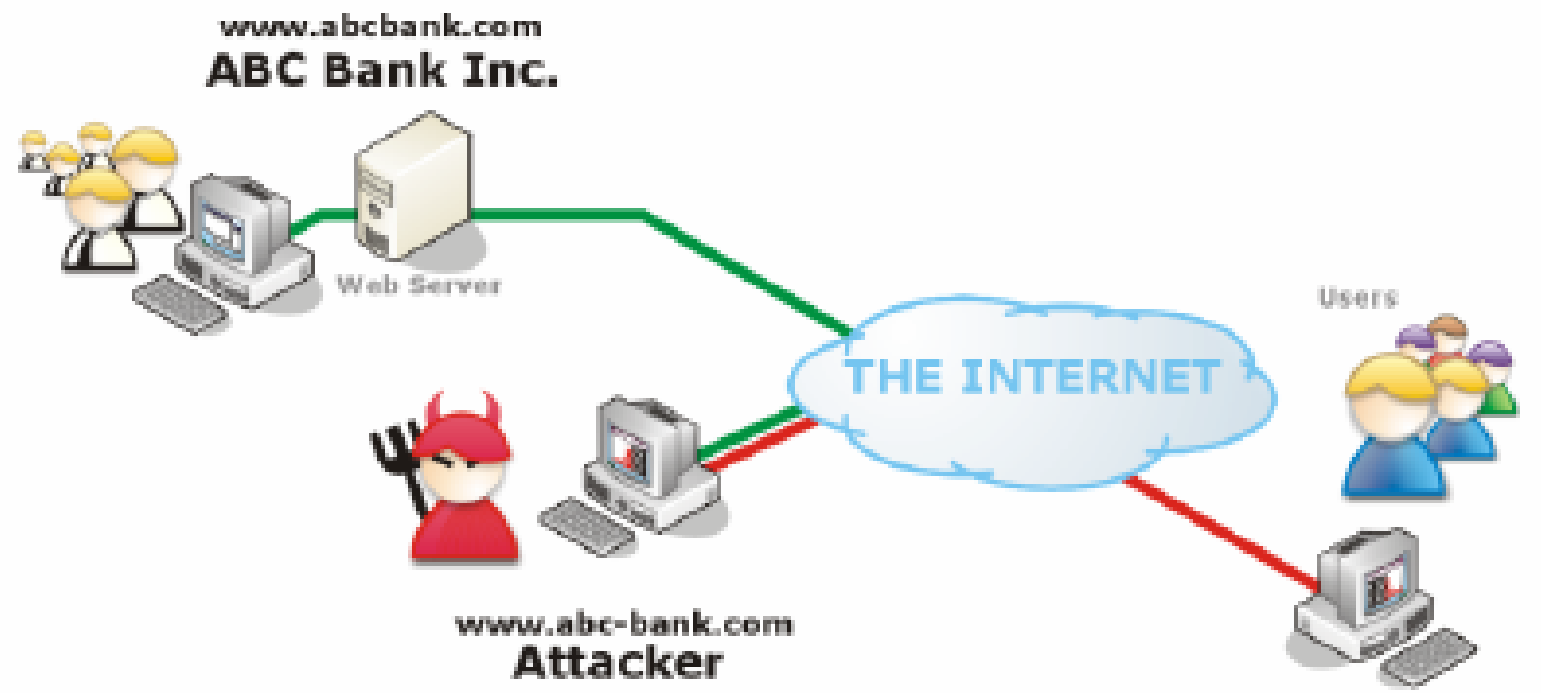


Man-in-the-middle-attack

Serangan aktif yang berbahaya



Man-in-the-middle attack di bidang *e-commerce*



With no entity authentication consumers have no ability to know if they are subject to a man-in-the-middle attack.

Jenis-jenis Serangan

Berdasarkan teknik yang digunakan untuk menemukan kunci:

1. *Exhaustive attack/brute force attack*
2. *Analytical attack*

1. Exhaustive attack /brute force attack

- Mengungkap plainteks dengan mencoba semua kemungkinan kunci

. Contoh: *dictionary attack*

- Pasti berhasil menemukan kunci jika tersedia waktu yang cukup dan sumberdaya *hardware* yang memenuhi.

Tabel 1 Waktu yang diperlukan untuk *exhaustive key search*
(Sumber: William Stallings, *Data and Computer Communication Fourth Edition*)

Ukuran kunci	Jumlah kemungkinan kunci	Lama waktu untuk 10^6 percobaan per detik	Lama waktu untuk 10^{12} percobaan per detik
16 bit	$2^{16} = 65536$	32.7 milidetik	0.0327 mikrodetik
32 bit	$2^{32} = 4.3 \times 10^9$	35.8 menit	2.15 milidetik
56 bit	$2^{56} = 7.2 \times 10^{16}$	1142 tahun	10.01 jam
128 bit	$2^{128} = 4.3 \times 10^{38}$	5.4×10^{24} tahun	5.4×10^{18} tahun

Solusi: Kriptografer harus membuat kunci yang panjang dan tidak mudah ditebak.

2. *Analytical attack*

- Menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.

- Caranya: memecahkan persamaan-persamaan matematika (yang diperoleh dari definisi suatu algoritma kriptografi) yang mengandung peubah-peubah yang merepresentasikan plainteks atau kunci.

- Contoh: Lihat kembali *Affine Cipher* ⟹ Enkripsi: $C \equiv mP + b \pmod{n}$
  Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n}$
  Kunci: m dan b

m bilangan bulat yang relatif prima dengan n
b adalah jumlah pergeseran

Ada 25 pilihan untuk b dan 12 buah nilai m yang relatif prima dengan 26 (yaitu 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, dan 25).

- Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack*.

- Solusi: kriptografer harus membuat algoritma kriptografi yang sekompleks mungkin

Jenis-jenis Serangan

- Berdasarkan ketersediaan data yang digunakan untuk menyerang sistem kriptografi:

1. *Chipertext-only attack*
2. *Known-plaintext attack*
3. *Chosen-plaintext* attack
4. *Adaptive-chosen-plaintext attack*
5. *Chosen-chipertext attack*

1. ***Chipertext-only attack***

   Kriptanalis hanya memiliki cipherteks

   Teknik yang digunakan: *exhaustive key search* dan teknik analisis frekuensi (akan dijelaskan kemudian)

   Diberikan: $C_1 = E_k(P_1), C_2 = E_k(P_2), \ldots, C_i = E_k(P_i)$

   Deduksi: $P_1, P_2, \ldots, P_i$ atau k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.

2. *Known-plaintext attack*

Diberikan sejumlah pasangan plainteks dan cipherteks yang berkoresponden:

$P_1, C_1 = E_k(P_1),$

$P_2, C_2 = E_k(P_2),$

$\ldots,$

$P_i, C_i = E_k(P_i)$

Deduksi: k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.

Beberapa pesan yang formatnya terstruktur membuka peluang untuk menerka plainteks dari cipherteks yang bersesuaian.

Contoh:

From dan *To* di dalam *e-mail*,

”Dengan hormat”, *wassalam*, pada surat resmi.

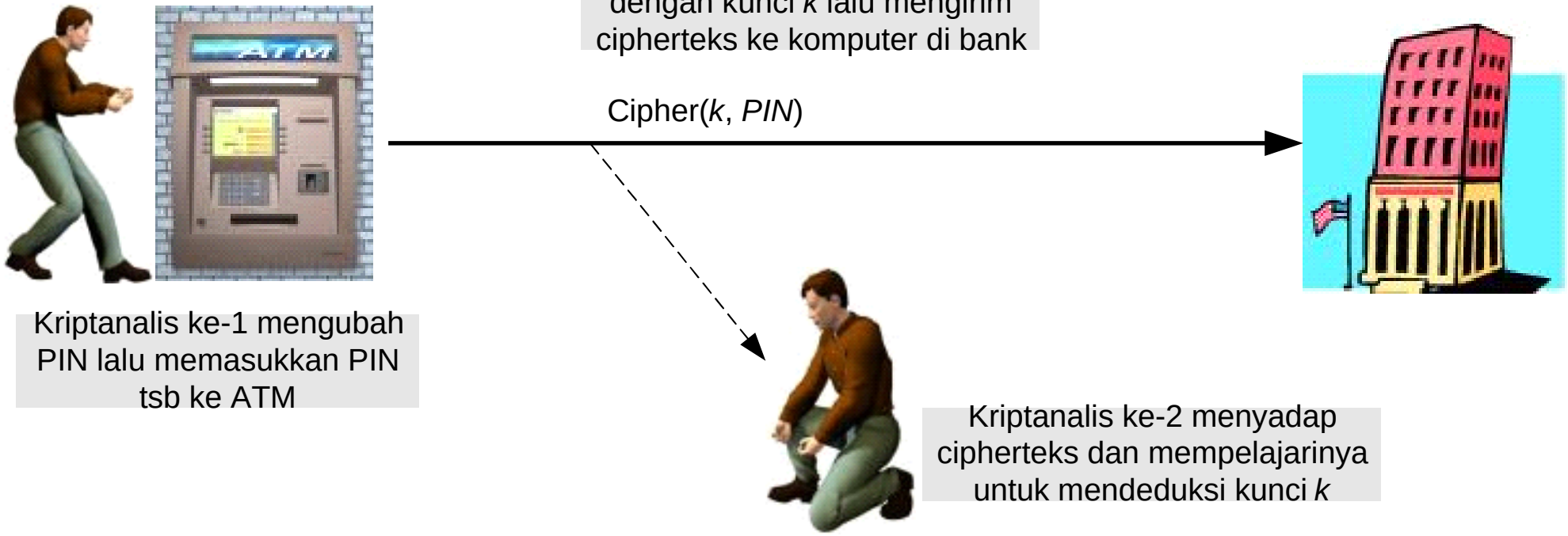
#include, *program*, di dalam *source code*

3. *Chosen-plaintext attack*

Kriptanalis dapat memilih plainteks tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

Diberikan: $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, \ C_i = E_k(P_i)$
di mana kriptanalis dapat memilih diantara $P_1, P_2, \ldots, P_i$

Deduksi: k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.



Chosen-plaintext attack

4. ***Adaptive-chosen-plaintext attack***

Kriptanalis memilih blok plainteks yang besar, lalu dienkripsi, kemudian memilih blok lainnya yang lebih kecil berdasarkan hasil serangan sebelumnya, begitu seterusnya.

5. Chosen-ciphertext attack

Diberikan:

$C_1, P_1 = D_k(C_1), C_2, P_2 = D_k(P_2), \ldots, C_i, P_i = D_k(C_i)$

Deduksi: *k* (yang mungkin diperlukan untuk mendekripsi pesan pada waktu yang akan datang).

Sebuah algoritma kriptografi dikatakan aman (*computationally secure*) bila ia memenuhi tiga kriteria berikut:

1. Persamaan matematis yang menggambarkan operasi di dalam algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.

2. Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.

3. Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.