

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!

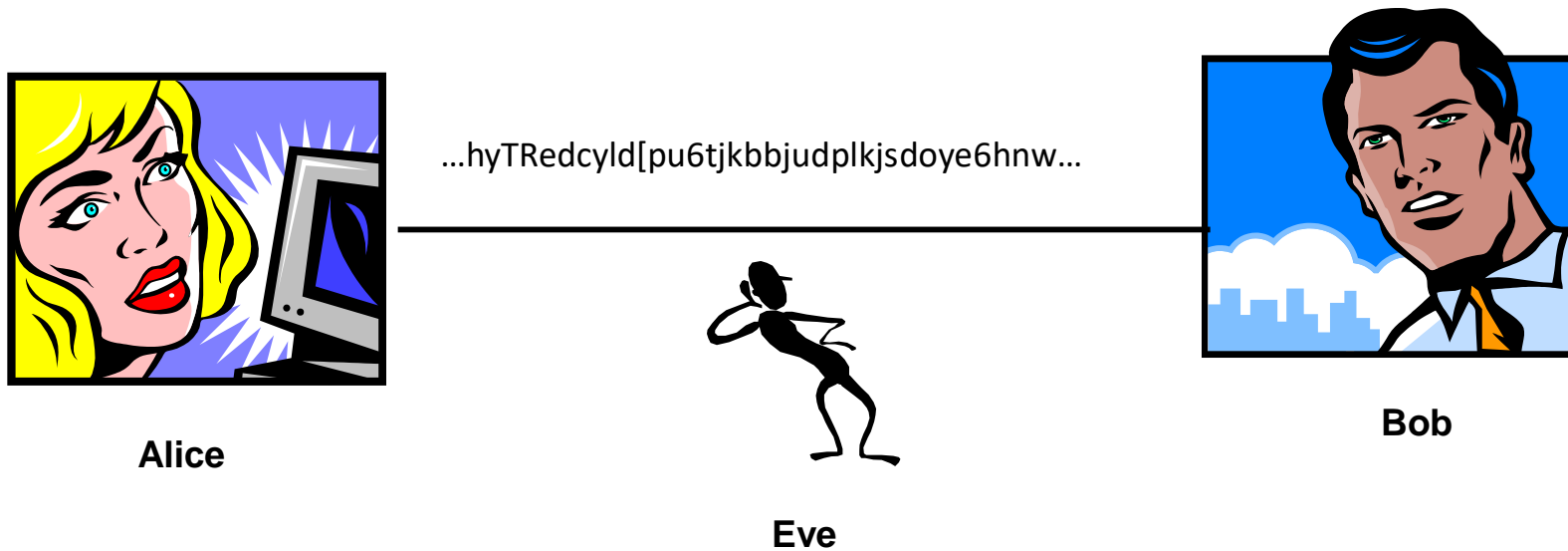
Jenis-jenis Serangan

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)

The screenshot shows the Wireshark interface with the following components:

- Window Title:** Capturing from Marvell Yukon Ethernet Controller (Microsoft's Packet Scheduler) : \Device\NPF_{55E0D470-0878-4504-A629-1...}
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help
- Filter:** Expression... Clear Apply Save
- Packet List Table:**

No.	Time	Source	Destination	Protocol	Length	Info
27	2.79561600	167.205.33.90	255.255.255.255	DB-LSP-	154	Dropbox LAN sync Discovery Protocol
28	2.96394400	167.205.33.14	167.205.33.255	NBNS	92	Name query NB CORPORATE<00>
29	3.06038000	00000000.00804837fc	00000000.ffffffff	NBIPX	98	Find name WORKGROUP<00>
30	3.06039600	4416db43.0000000000	00000000.00804837fc	NBIPX	98	Name recognized WORKGROUP<00>
31	3.06809700	167.205.33.14	167.205.33.255	NBNS	92	Name query NB CORPORATE<00>
32	3.09102200	167.205.33.88	167.205.33.255	NBNS	92	Name query NB PRINTERBASDAD<00>
33	3.24244300	AsustekC_10:09:66	Broadcast	ARP	60	who has 167.205.33.12? Tell 167.205.33.2
34	3.30945700	Cisco-Li_11:0d:0f	Spanning-tree-(for- STP		60	RST. Root = 32768/0/00:22:6b:10:d8:3d Co
35	3.35738600	167.205.33.121	167.205.33.255	NBNS	92	Name query NB SUDARMAN<20>
36	3.47038100	167.205.33.61	50.62.3.118	TCP	62	mctet-gateway > https [SYN] Seq=0 win=655
37	3.60684800	IntelCor_c2:e0:11	Broadcast	ARP	60	who has 167.205.33.116? Tell 167.205.33.:
38	3.71257800	167.205.33.14	167.205.33.255	NBNS	92	Name query NB CORPORATE<00>
39	3.80628200	167.205.33.14	167.205.33.255	NBNS	92	Name query NB CORPORATE<00>
40	3.83975500	00000000.00804837fc	00000000.ffffffff	BROWSEF	176	Request Announcement DAPUR
41	3.83996700	167.205.33.100	167.205.33.255	BROWSEF	243	Host Announcement BUGI-WIBOWO, workstatio
- Packet Details:**
 - Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 - IEEE 802.3 Ethernet
 - Logical-Link Control
 - Internetnetwork Packet exchange
 - NetBIOS over IPX
- Packet Bytes:**

0000	ff ff ff ff ff ff 00 80	48 37 fc 30 00 54 e0 e0	H7.0.T..
0010	03 ff ff 00 50 00 14 00	00 00 00 ff ff ff ff ffP...
0020	ff 04 55 00 00 00 00 00	80 48 37 fc 30 04 55 00	..U.....	.H7.0.U.
0030	03 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 c0
0050	02 01 02 5f 5f 4d 52 42	52 4f 57 52 45 5f 5f 02	MSP POWER

At the bottom, the status bar shows: Marvell Yukon Ethernet Controller (Microsoft's Pa... | Packets: 729 Displayed: 729 Marked: 0 | Profile: Default

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
1034	8.148165	172.99.96.253	160.153.129.234	HTTP	617	POST /sign

[Full request URI: http://www.sababank.com/signin.php]
 [HTTP request 1/1]
 [Response in frame: 1129]
 File Data: 53 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "username" = "Ibrahim_Diyeb"
- Form item: "password" = "yemen_123"
- Form item: "actn" = "signin"

01a0	63 6f 64 65 64 0d 0a 43	6f 6e 74 65 6e 74 2d 4c	coded..Content-L
01b0	65 6e 67 74 68 3a 20 35	33 0d 0a 43 6f 6f 6b 69	ength: 5 3..Cooki
01c0	65 3a 20 50 48 50 53 45	53 53 49 44 3d 34 31 32	e: PHPSESSID=412
01d0	33 35 34 31 32 30 63 35	36 37 34 35 61 63 66 34	354120c5 6745acf4
01e0	31 62 38 65 32 39 36 34	63 32 62 65 35 3b 20 6c	1b8e2964 c2be5; l
01f0	61 6e 67 3d 61 72 61 62	69 63 0d 0a 43 6f 6e 6e	ang=arabic..Conn
0200	65 63 74 69 6f 6e 3a 20	6b 65 65 70 2d 61 6c 69	ection: keep-ali
0210	76 65 0d 0a 55 70 67 72	61 64 65 2d 49 6e 73 65	ve..Upgrade-Inse
0220	63 75 72 65 2d 52 65 71	75 65 73 74 73 3a 20 31	ure-Req uests: 1
0230	0d 0a 0d 0a 75 73 65 72	6e 61 6d 65 3d 49 62 72	...user name=Ibr
0240	61 68 69 6d 5f 44 69 79	65 62 26 70 61 73 73 77	ahim_Diy eb&passw

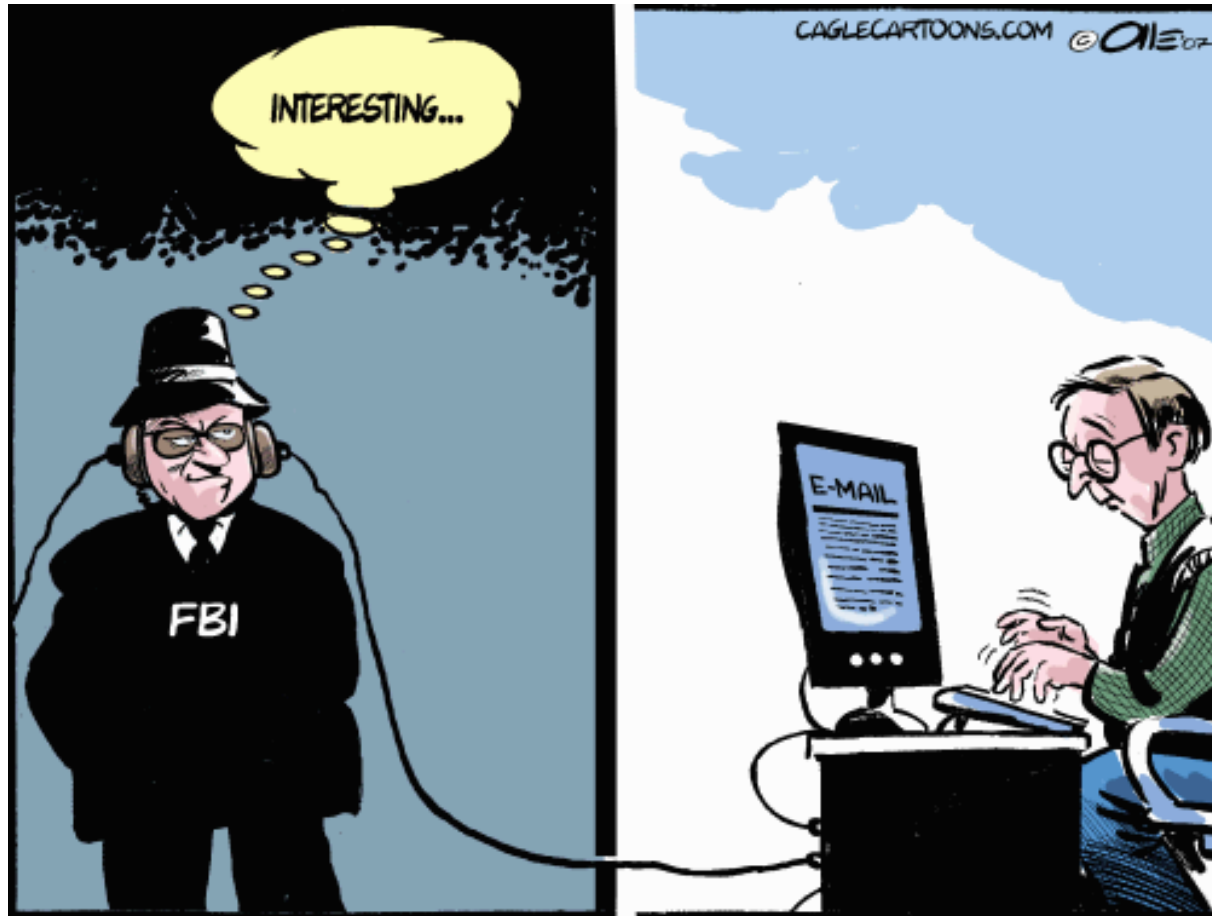
Filtering dengan Wireshark dapat menampilkan plainteks berupa *username* dan *password*

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

Metode penyadapan:

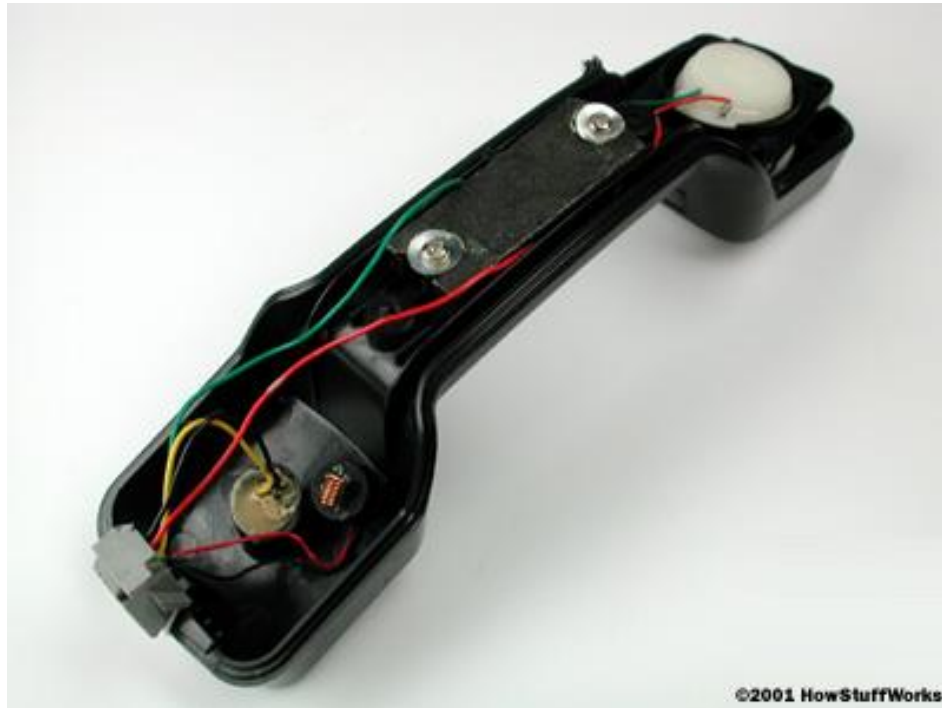
1. *Wiretapping*
2. *Electromagnetic eavesdropping*
3. *Acoustic Eavesdropping*

- *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



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

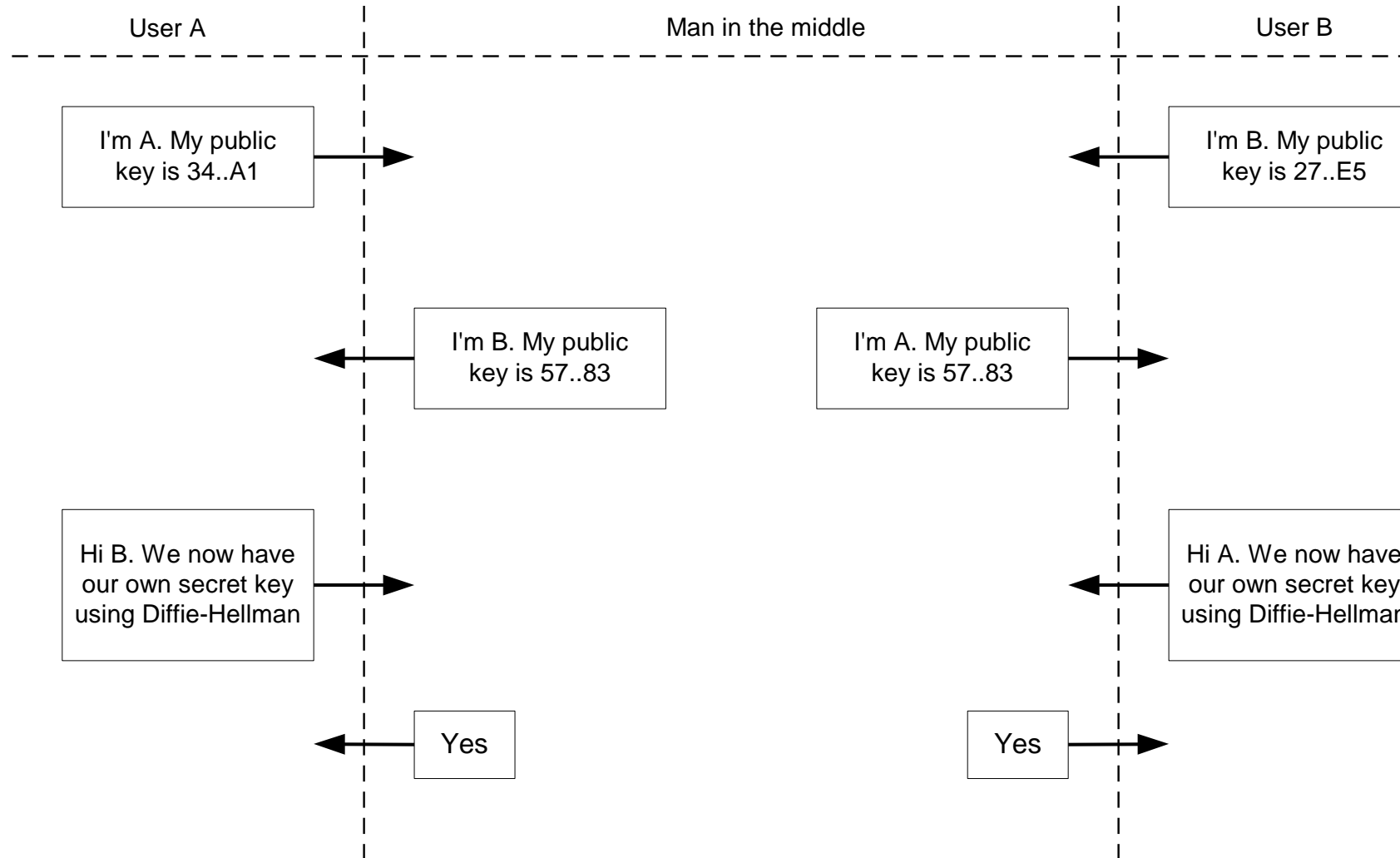
Creatas

www.comstock.com

2. Serangan aktif (*active attack*)

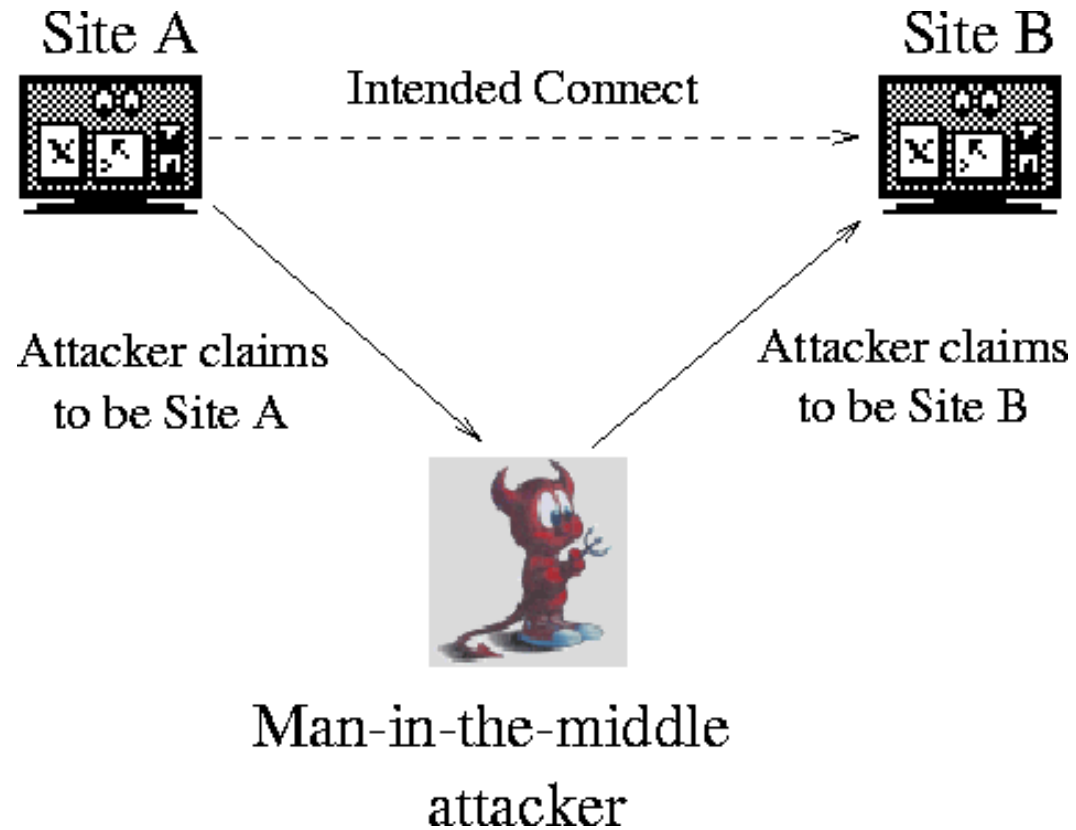
- penyerang mengintervensi komunikasi dan ikut mempengaruhi system untuk keuntungan dirinya
- penyerang mengubah aliran pesan seperti:
 - menghapus sebagian cipherteks,
 - mengubah cipherteks,
 - menyisipkan potongan cipherteks palsu,
 - *me-replay* pesan lama,
 - mengubah informasi yang tersimpan, dsb
- Contoh: *man-in-the-middle attack*

Man-in-the-middle-attack

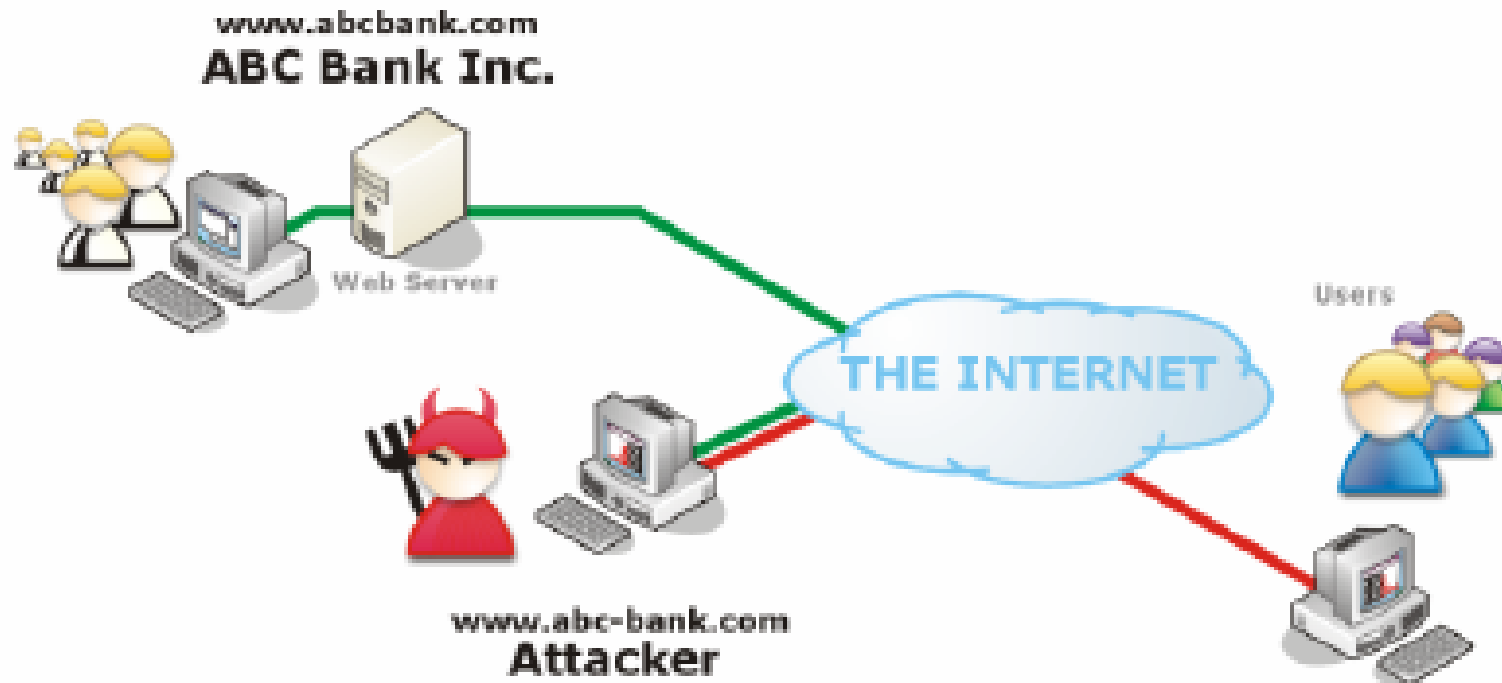


Man-in-the-middle-attack

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***

Kriptanalisis hanya memiliki cipherteks

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

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

Deduksi: P_1, P_2, \dots, 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:

$$P_1, C_1 = E_k(P_1),$$

$$P_2, C_2 = E_k(P_2),$$

...

$$P_i, C_i = E_k(P_i)$$

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.

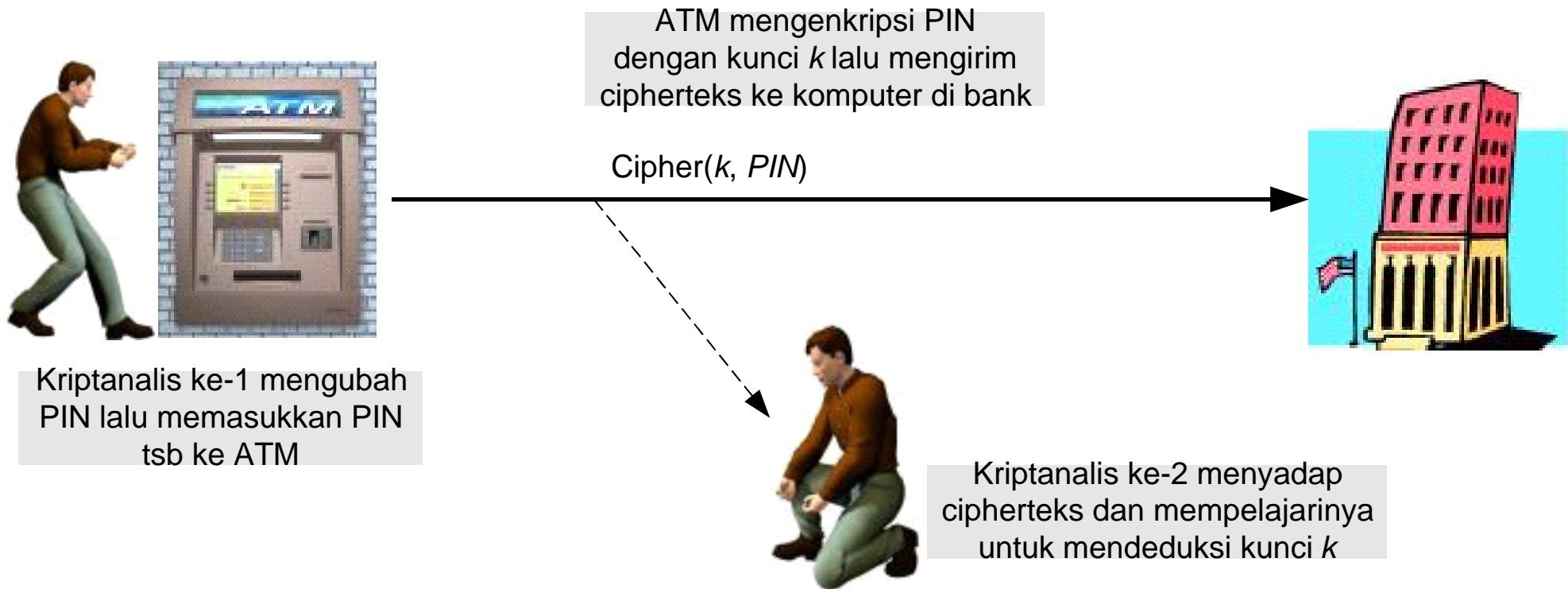
#include, program, di dalam *source code*

3. *Chosen-plaintext attack*

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

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

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

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.