Keamanan Jaringan

36. Kajian 2

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Defense

Kajian	Kompetensi Dasar	Kompetensi Menengah	Kompetensi Mahir
Teknik Pengamanan jaringan	Mengetahui teknik pengamanan jaringan	Mampu melakukan & membedakan teknik-teknik pengamanan	Mampu merancang sistem keamanan

Materi Kajian 2

Autentikasi

DMZ

Cryptography

IPS

VPN

Firewall

IDS

Cryptography

- **Cryptography** (*cryptology*; dari bahasa Yunani κρυπτός, “rahasia";γράφειν, *graphein*,“menulis", λογία, -*logia*, “ilmu“)
- Ilmu untuk menulis/membuat pesan rahasia

Kenapa Rahasia?

- Militer
- Diplomat
- Pejabat negara
- Perang

Implementasi Kriptografi

- Transaksi e-banking
- Password
- Kartu Kredit
- Digital Currency
- Digital Signature

Keamanan Jaringan

37. Sejarah Kriptografi

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Enigma Rotor

- Digunakan Jerman pada Perang Dunia 2
- Memiliki rotor yang berubah posisinya setelah setiap huruf dikirim
- Mengacak pesan rahasia
- Dikirimkan melalui Radio
- 158.962,555,217,826,360,000 = 159 quintillion

The Bombe

- Mesin
- Marian Rejewski
- Alan Turing
- Gordon Welchman

Code Talker

- Diterjemahkan ke Bahasa yang unik
- Amerika : WW1 dan WW2
- Bahasa suku Indian
- Cherokee dan Choctaw
- 500 orang → US Marine

The Codebreakers

- David Kahn
- Sejarah Kriptografi
- Mesir Kuno
- 1967

BSSN

- Badan Siber dan Sandi Negara
- Lembaga Sandi Negara
- Algoritma
- Perangkat

Keamanan Jaringan

38. Kriptografi Klasik

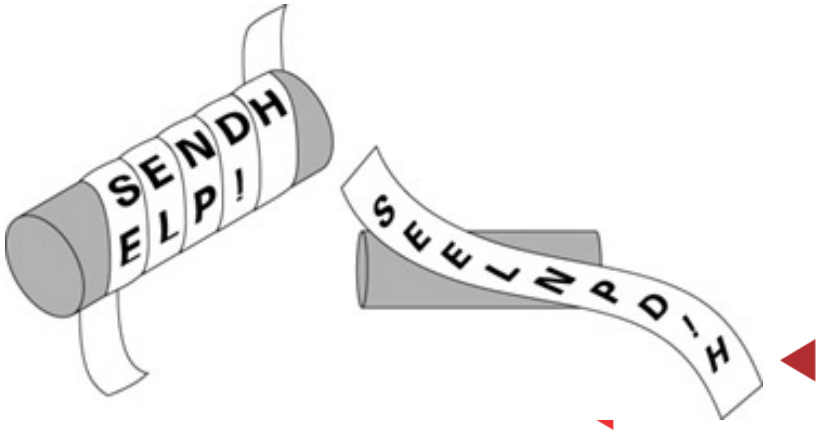
Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Transposisi

- Mengacak Urutan Huruf
- Yunani →scytale
- Kayu → Diameter yang Sama
- SEND HELP!
- SEELNPD!H



Transposisi menggunakan Tabel

1. Pesan

K	I	R	I	M	B	A	N	T	U	A	N	S	E	G	E	R	A

2. Kode

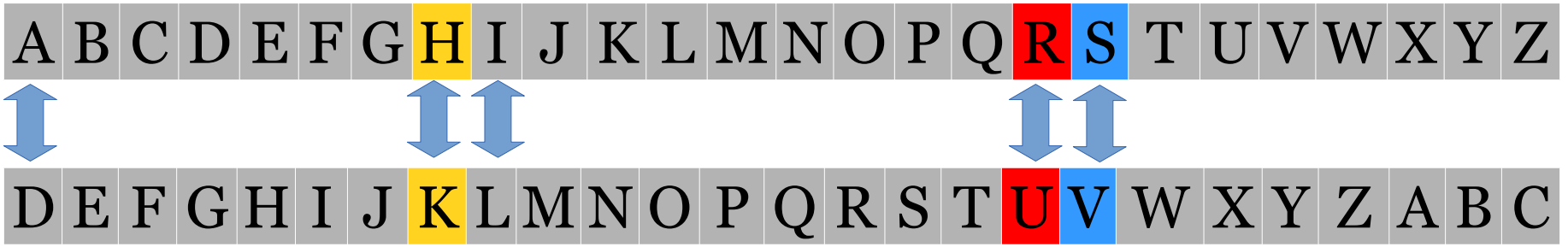
K	I	A	U	S	E	I	M	N	A	E	R	R	B	T	N	G	A

3. Tabel Transposisi

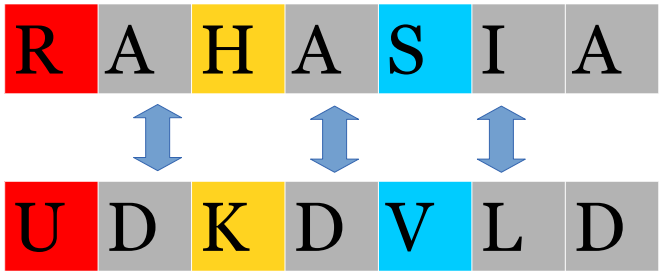
K	I	A	U	S	E
I	M	N	A	E	R
R	B	T	N	G	A

Substitusi

- Mengganti pesan dengan urutan lain

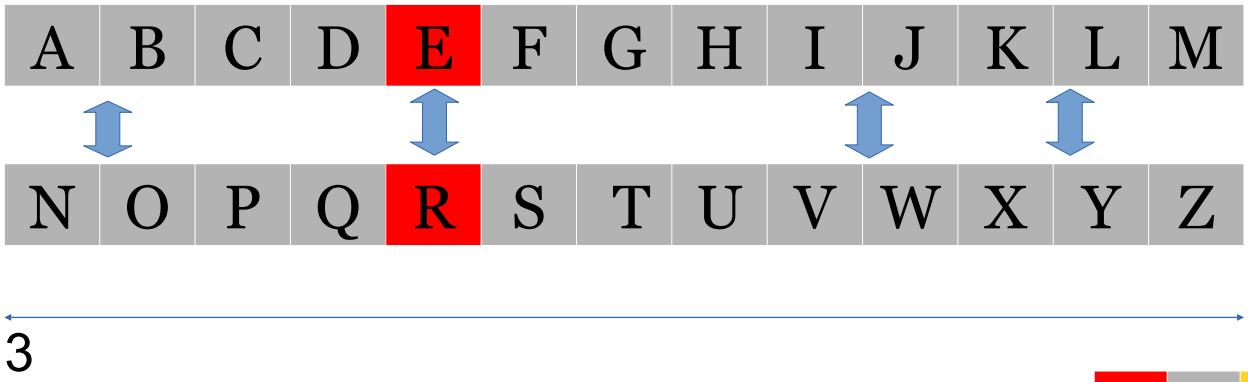


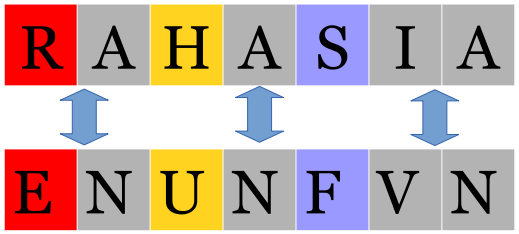
- Caesar Cipher – Geser 3



ROT 13

- Menggeser huruf sebanyak 13 huruf
- www.rot13.com





CIPHER dgn Banyak Tabel

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
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
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
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

- Huruf Pertama dengan tabel pertama
- Huruf Kedua dengan tabel kedua
- Huruf ketiga dengan tabel ketiga
- Huruf Keempat dengan tabel keempat

R	A	H	A	S	I	A
R	D	N	J	S	L	G

Keamanan Jaringan

39. Komponen Kriptografi

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Komponen Kriptografi

- *Plain Text*
- Sumber berita / pesan / Teks asli
- *Cipher Text*
- Text yang sudah diproses diacak digantikan
- *Algoritma & Kunci*
- Bagaimana pesan diubah, contoh substitusi

Perubahan Pesan Menjadi Kode

Enkripsi

- Proses merubah pesan menjadi kode
- Plain Text → Cipher Text

Dekripsi

- Proses mengembalikan kode menjadi pesan
- Cipher Text → Plain Text

Algoritma Klasik

- Transposisi
- Substitusi : Caesar Cipher
- Kautiliyam dan Mulavediya : India
- Sah-Dabiriya & raz-sahariya : Persia
- Frequency Analysis: Al-Kindi → permutasi & Kombinasi
- Polyalphabethic Cipher: Al-Qalqashandi →Viginere

Kripto Berdasarkan Tipe Input Data

- **Block Cipher**
  - Enkripsi dilakukan pada setiap blok data input
  - 1 blok = 64 bits, 128 bits

- **Stream Cipher**
  - Enkripsi dilakukan langsung

Jenis Kriptografi Berdasarkan kunci

- ***Private key Cryptosystem / kunci privat***
  - Simetrik (kunci untuk mengunci dan membuka sama/ satu)
- ***Public Key Cryptosystem / kunci publik***
  - Asimetrik (kunci untuk mengunci dan membuka berbeda)

Keamanan Jaringan

40 Algoritma Simetris

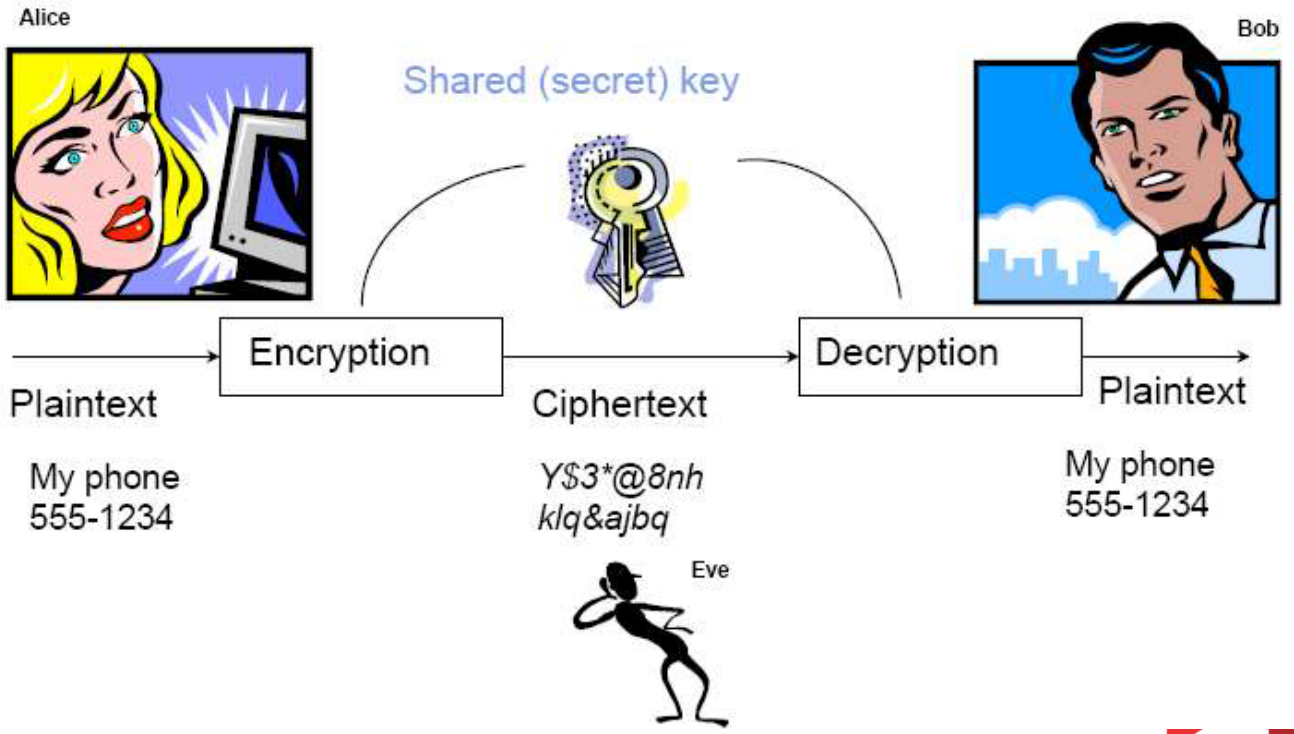
Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Kriptografi Kunci Privat

- Kunci enkripsi = kunci dekripsi



Siapa Bob dan Alice

- 2 pihak yang ingin berkomunikasi!
- Web browser/server untuk transaksi
- elektronik (contohnya e-commerce)
- on-line banking client/server
- DNS servers
- Antar router
- dll

Kriptografi Kunci Privat

Menggunakan satu kunci yang sama pada saat Enkripsi dan dekripsi

1) Masalah dalam distribusi kunci
   - butuh saluran khusus
   - Jumlah kunci sangat banyak

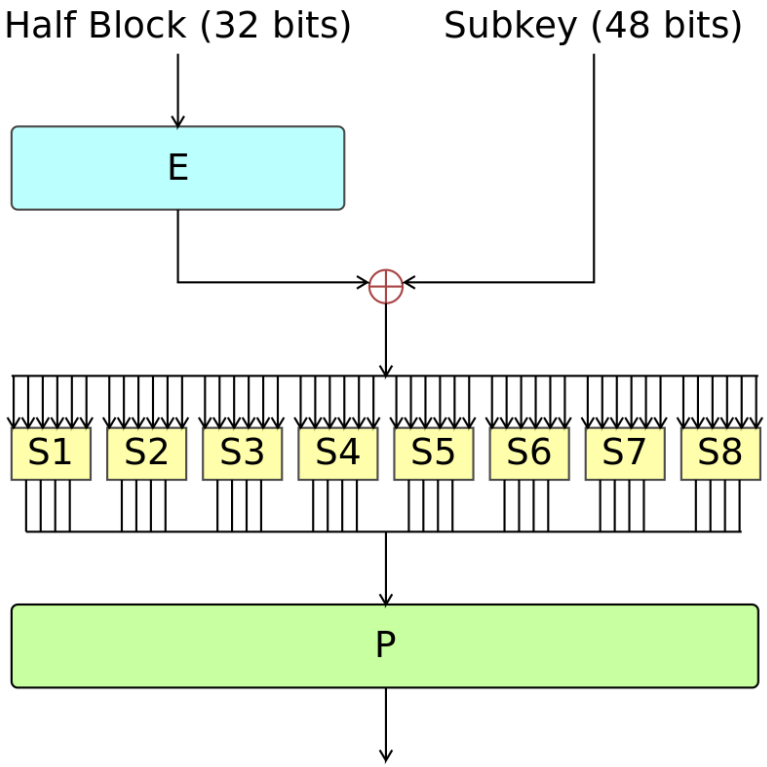
2) Keuntungan Operasi Cepat

Algoritma Simetrik

- Twofish
- Serpent
- AES
- Blowfish
- CAST5
- Kuznyechick
- RC4
- DES
- 3DES
- Skipjack
- Safer
- IDEA

Data Enrycption Standard (DES)

- Data 64 Bits
- Kunci 54 bit
- Block Chiper
- USA - 1977
- 3DES, AES



Keamanan Jaringan

34. XSS Attack

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

AES

- Adcanced Encryption Standard
- NIST (National Institute of Standard & Technology)
- 2001 –USA
- Pengganti DES

Kompetisi Terbuka

- US NIST call for cipher → 1997
- Kompetisi Terbuka
- 15 kandidat diterima Juni 1998
- Diuji :
  - Keamanannnya
  - Performansi di Arsitektur berbeda
  - Smart Card, FPGA

Finalis

- 1999: 5 Finalis
- MARS, RC6, Rijndael, Serpent dan twofish
- 2000: Rijndael
- Standar dokumen pemerintah USAS
- Apresiasi Komunitas
- Bruce Schneier (Twofish): *“I have nothing but good things to say about NIST and the AES process“*

Rijndael

- Vincent Rijmen dan Joan Daemen
- 8 bit
- Finite Field Arithmetic
- 1 blok 128 bit; panjang kunci 128, 192 dan 256
- Substitusi & Permutasi
- Pengulangan 10 ronde→ 128 bit; 12→ 192; 14→256

Implementasi AES

- RAR, Winzip, 7z
- NTFS
- Bitlocker, Truecrypt
- IEEE 802.11 Wireless
- Whatsapp, Facebook Messenger
- IPSec → VPN
- GPG →
- Intel & AMD Processor
- Grand Theft Auto

Keamanan Jaringan

45. Keamanan Algoritma Simetris

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

BruteForce

- Mencoba semua kombinasi kunci
- Perlu Komputasi besar
- 128 bit kunci AES →1×10^{18} tahun
- 256-bit → $3{,}31 \times 10^{56}$ tahun
- Supercomputer

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Teknik Serangan

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext
- Chosen-ciphertext attack
- Chosen-key attack
- Adaptive chosen-plaintext attack
- Timing attack
- Rubber hose attack

Cryptanalis

- 2002; XSL attack;
- Theoretical attack ; Courtois dan Pieprzyk → tidak berhasil
- 2009: Alex Biryukov, Dmitry Khovratovich, dan Ivica Nikolić,
- 2011; Bogdanov, Khovratovich, dan Rechberger,
- Snowden; NSA melakukan percoban menggunakan TAU statistik
- Tanpa kunci→ belum ada yang berhasil (bila implementasi benar)

Side Channel Attack

1. Kelemahan pada implementasi
2. Hardware/Software
3. Mengukur pemakaian energi
4. Emisi elektromagnet
5. Panas yang dihasilkan
6. Butuh akses ke perangkat

Tools

- Cryptool
- Cryptobench
- Jipher
- Ganzua
- Crank
- Evercrack

- AplhaPeeler
- DraftCryptoAnalyzer
- Linear Hull Cryptanalysis
- Mediggo
- subcypher

Terima Kasih

Materi Berikutnya:

Kajian 2
Kriptografi Algoritma Kunci Publik

Referensi

Buku Bacaan Wajib (BW)

Singh, S. (1999). *Code Book- The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchorbooks.

Stallings, W. (2010). *Network Security Essentials:Applications and Standards 4th Edition*. Prentice Hall.

Buku Bacaan Anjuran (BA)

Harris, S. (2010). *CISSP All in One Exam Guide, 5th Edition*. McGraw Hill.