Keamanan Siber
Cryptography

Always The First

Pengamanan Data

- Steganography
  - Menyembunyikan pesan dalam media yang terlihat biasa
  - Membuat seolah-olah tidak ada pesan
- Cryptography
  - Membuat pesan agar tidak mudah dibaca/dimengerti

Steganography

- Physical Steganography
  - –Jaman Yunani kuno: pesan disembunyikan diatas meja yang dilapisi lilin
  - –Pesan ditato di kulit kepala para budak
- Printed Steganography
  - –Pesan terkandung dalam tulisan
  - –Contoh: hanya dengan mengambil huruf depan setiap kata dalam sebuah paragraf, membentuk sebuah pesan

Steganography

- Digital Steganography
  - Pesan diletakkan dalam file, umumnya file gambar atau suara
  - Digital watermarking
- Network Steganography
  - Pesan rahasia diletakkan dalam header paket data
  - Pesan rahasia diletakkan dalam corrupt paket, hanya dibaca oleh protokol tertentu (HICCUPS System)

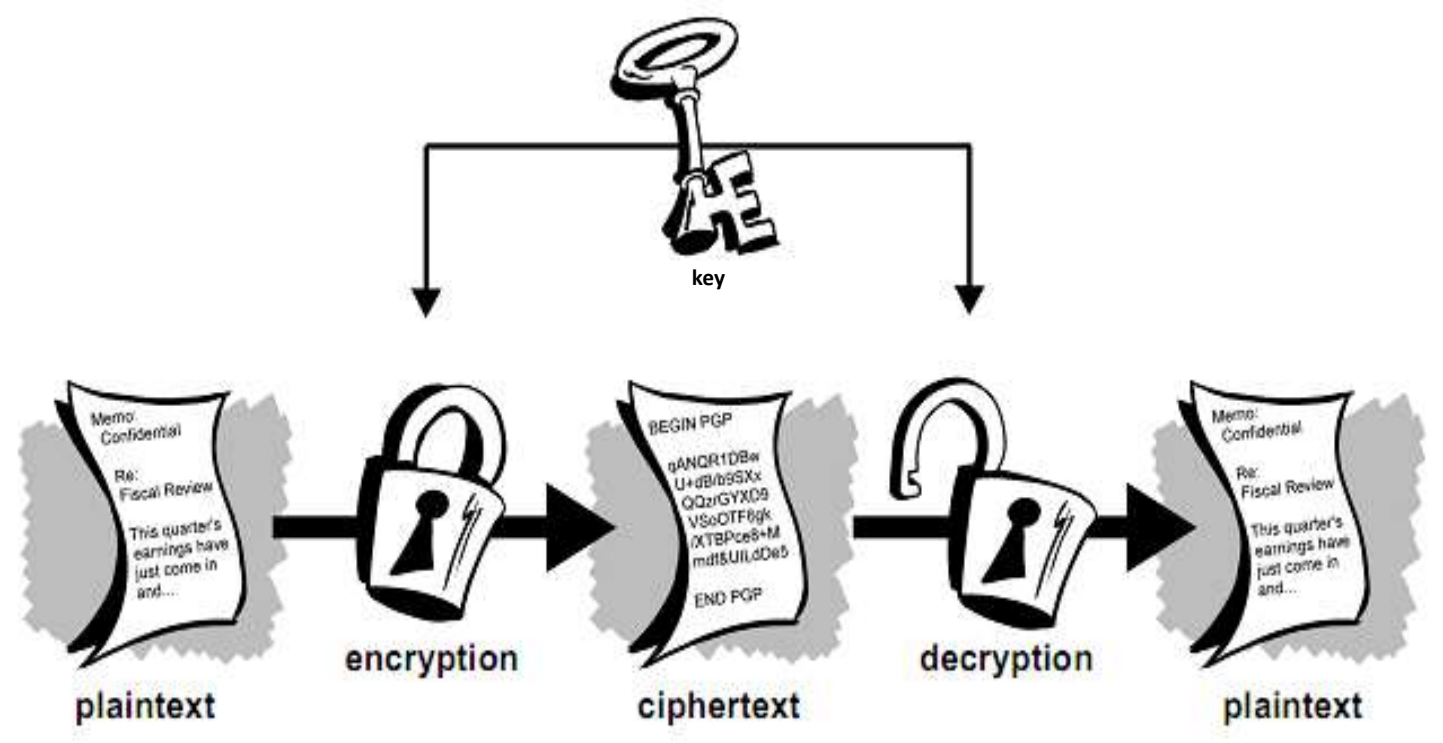
Criptology

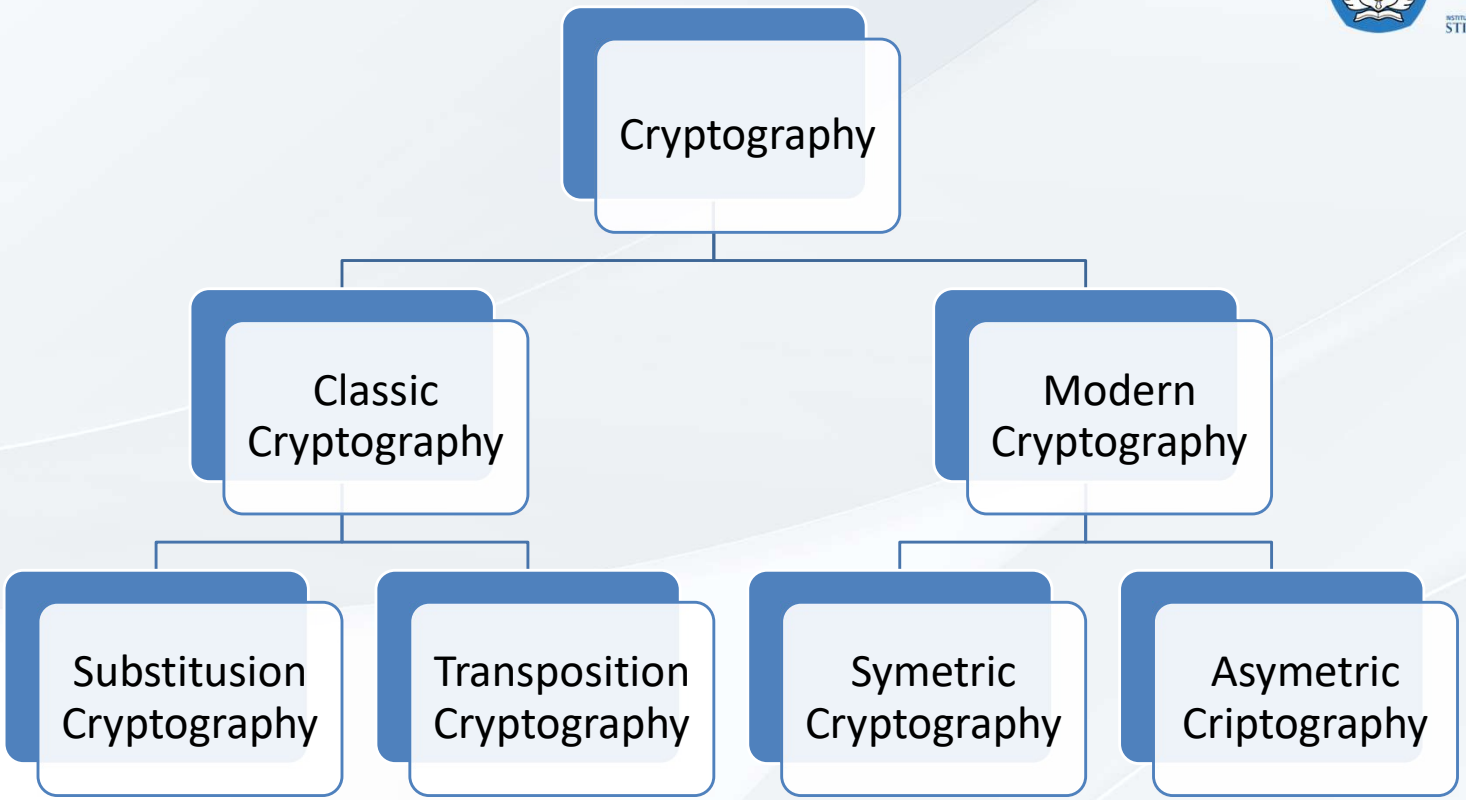
- Cryptography
  - Teknik menyembunyikan informasi agar tidak mudah dimengerti
  - Pelaku : Cryptographer
- Cryptanalysis
  - Teknik mendapatkan informasi dari suatu pesan terenkripsi, tanpa mengetahui komponen rahasianya (kunci, algoritma)
  - Pelaku : Cryptanalyst

Elemen Cryptography

- Informasi
  - Plaintext : teks asli
  - Ciphertext : teks yang disembunyikan
- Method / Algoritma / Cipher
  - Encryption / encipher : proses menyembunyikan teks
  - Decryption / decipher: proses mengembalikan ke teks asli
- Kunci / Key

Cryptography




Cryptography
Classic Cryptography
Modern Cryptography
Substitusion Cryptography
Transposition Cryptography
Symetric Cryptography
Asymetric Criptography

Classic Cryptography

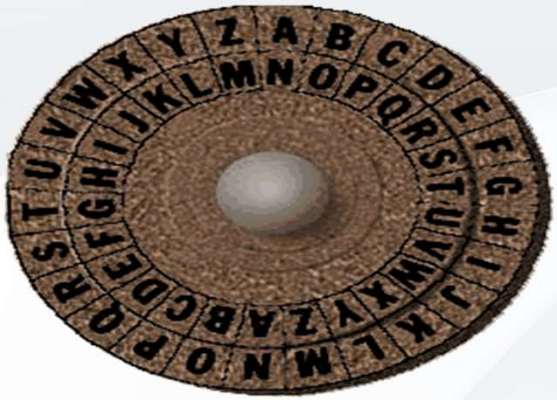
Always The First

Classic Cryptography

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena, kertas, mesin mekanik atau alat sederhana lainnya
- Digunakan saat perang agar pesan tidak jatuh ke tangan musuh
- Algoritma kriptografi klasik:
  - Substitution Ciphers
  - Transposition Ciphers

Classic Cryptography

Spartan Scytale



Caesar Cipher Disk

Enigma Machine

Always The First

Substitution Ciphers

- Algoritma enkripsi dengan menggantikan satu karakter dengan karakter lainnya
- Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext
- Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext

Caesar Cipher

- Monoalphabetic Substitution Cipher
- Digunakan oleh Julius Caesar
- Tiap huruf alfabet digeser sejumlah `n`.
  Key = n

Geser 3 || key = 3

Pt	A	B	C	D	E	F	G	H	I	..	..	W	X	Y	Z
Ct	D	E	F	G	H	I	J	K	L	..	..	Z	A	B	C

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBD REHOLA**

Always The First

Caesar Cipher

- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

  DZDV LDVW HULA GDQW HPDQ QBAR EHOL A

- Atau membuang semua spasi:

  DZDVLDVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit

Vigènere Cipher

- Polyalphabetic Substitution Cipher
- Menggunakan Tabel Vigènere untuk melakukan enkripsi
- Setiap baris di dalam bujursangkar menyatakan huruf-huruf ciphertext
- Baris horizontal atas adalah plaintext
- Kolom vertikal kiri adalah key
- Huruf ciphertext diperoleh dengan memotongkan huruf plaintext dengan huruf key

P L A I N T E X T

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	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
G	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
H	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	G
I	I	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
J	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
K	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	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
W	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Vigènere Cipher

- Contoh penerapan Vigènere Cipher :

  Plaintext : THISPLAINTEXT

  Kunci : sonysonysonys

  Cipherteks : **LVVQHZNGFHRVL**

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Dalam hal ini Kunci "sony" diulang sebanyak panjang plaintext-nya

Transposition Ciphers

- Algoritma enkripsi dengan mengubah posisi huruf di dalam plaintext
- Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian huruf di dalam plaintext
- Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut

Transposition Ciphers

- Contoh 1:
  - Plaintext :

    STIKOM BALI ALWAYS THE FIRST
  - Encryption :

    STIKOM

    BALIAL

    WAYSTH

    EFIRST
  - Ciphertext (dibaca secara vertikal) :

    SBWETAAFILYIKISROATSMLHT

Transposition Ciphers

- Contoh 2:
  - Plaintext :
    STIKOM BALI ALWAYS THE FIRST
  - Encryption :
    STIKOM
    BALIAL
    WAYSTH
    EFIRST
  - Ciphertext (dibaca secara diagonal) :
    MOLHAKIITTSSLTSAYRIABWFE

Transposition Ciphers

- Contoh 3:
  - Plaintext :

    STIKOM BALI ALWAYS THE FIRST
  - Encryption : key = 532614

    STIKOM BALIAL WAYSTH EFIRST

    123456 123456 123456 123456
  - Ciphertext :

    OITMSKALALBITYAHWSSIFTER

Modern Cryptography

Always The First

Modern Cryptography

- Tetap menggunakan gagasan pada algoritma klasik: substitusi dan transposisi, tetapi lebih rumit
- Perkembangan algoritma kriptografi modern didorong oleh penggunaan komputer digital untuk keamanan pesan
- Komputer digital merepresentasikan data dalam biner
- Semua elemen kriptografi direpresentasikan dalam bentuk bit (0, 1)

Modern Cryptography

- Beroperasi dalam mode bit
  - –kriptografi klasik beroperasi dalam mode karakter
  - –kunci, plainteks, cipherteks, diproses dalam rangkaian bit
  - –operasi bit xor paling banyak digunakan

XOR – Exclusive Or

- Simbol / Notasi : $\oplus$
- Hukum :
  - $a \oplus a = 0$
  - $a \oplus b = b \oplus a$
  - $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- Dalam kriptografi, menggunakan bitwise operation
  - Operasi dilakukan tiap satu bit

Klasifikasi

- Symmetric Algorithm
  - –Block Chiper
  - –Stream Chiper
- Asymmetric Algorithm
- Hash Function

Symmetric Algorithm

- Algoritma kriptografi yang menggunakan kunci yang sama untuk enkripsi dan dekripsi
- Sebutan lain:
  - –symmetric-key
  - –secret-key
  - –single-key
  - –shared-key
  - –one-key
  - –privat-key

Block Cipher

- Pesan (dalam bentuk rangkaian bit) dipecah menjadi beberapa blok

  Contoh:

  Plainteks:

  100111010110

  Jika dibagi menjadi blok 4-bit:

  1001 1101 0110

  Maka setiap blok menyatakan 0 - 15:

  9 13 6

Padding Bits

- bit-bit tambahan jika ukuran blok terakhir tidak mencukupi panjang blok

  Contoh:

  Plainteks: 100111010110

  Bila dibagi menjadi blok 5-bit:

  10011 10101 00010

mengakibatkan ukuran plainteks hasil dekripsi lebih besar daripada ukuran plainteks semula.

Hexadecimal

- Pada beberapa algoritma kriptografi, pesan dinyatakan dalam kode Hexadecimal (Hex)

  Contoh: 100111010110

  Blok 4 bit: 1001 1101 0110

  Kode Hex: 9 D 6

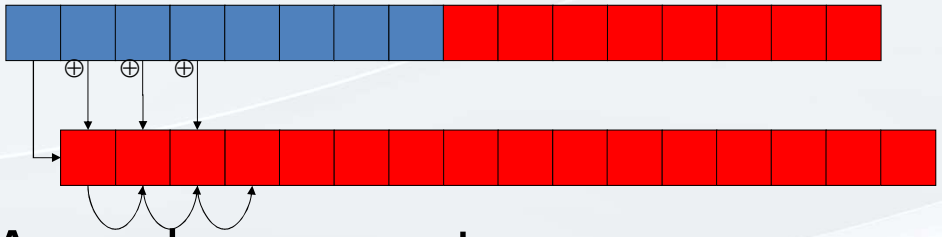
Kode hex digunakan pada blok kelipatan 4

Stream Cipher

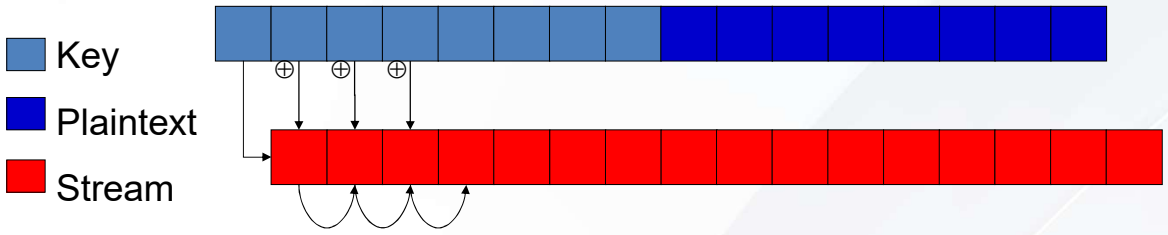
- Kunci digunakan sebagai “seed” untuk membuat stream
- Stream dikombinasikan dengan plaintext untuk menghasilkan ciphertext
- Kalsifikasi stream:
  - Synchronous stream:
    stream tidak tergantung pada plaintext
  - Asynchronous stream:
    stream tergantung pada plaintext

Stream

- Synchronous stream
  - Contoh:



- Asynchronous stream
  - Contoh:



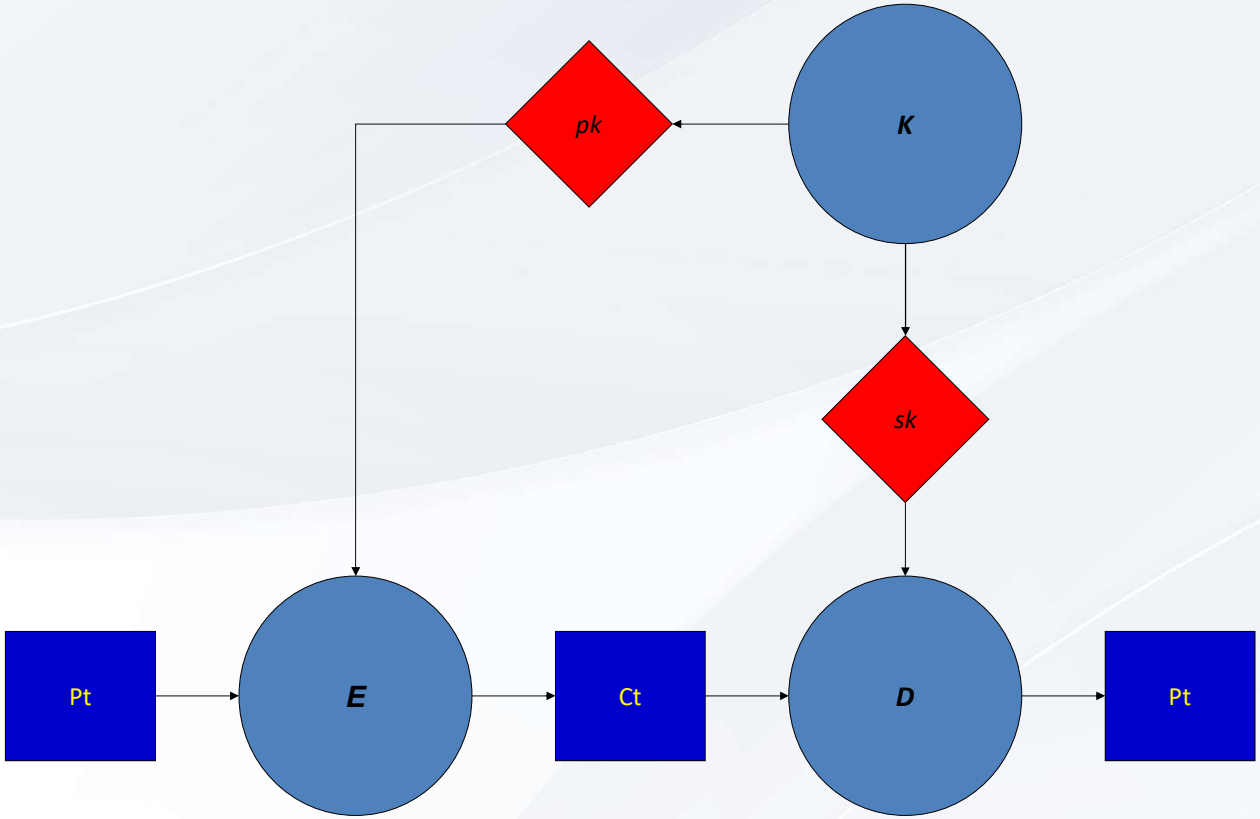
Contoh Algoritma Simetri

- Blok Chiper
  - –DES
  - –IDEA
  - –AES
- Stream Chiper
  - –OTP
  - –A5
  - –RC4

Asymmetric Algorithm

- Menggunakan kunci yang berbeda untuk enkripsi dan dekripsi
  - –Public Key → Enkripsi
  - –Private Key (Secret Key) → Dekripsi
- Muncul untuk mengatasi permasalahan penyampaian kunci ke penerima pesan
- Sebutan lain:
  - –Public-key Algorithm

Skema Algoritma

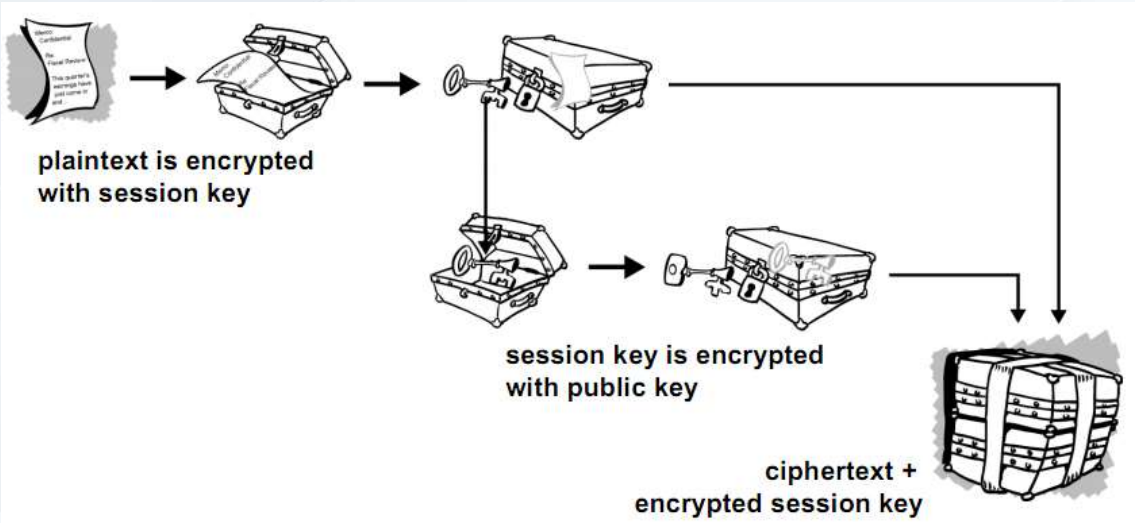


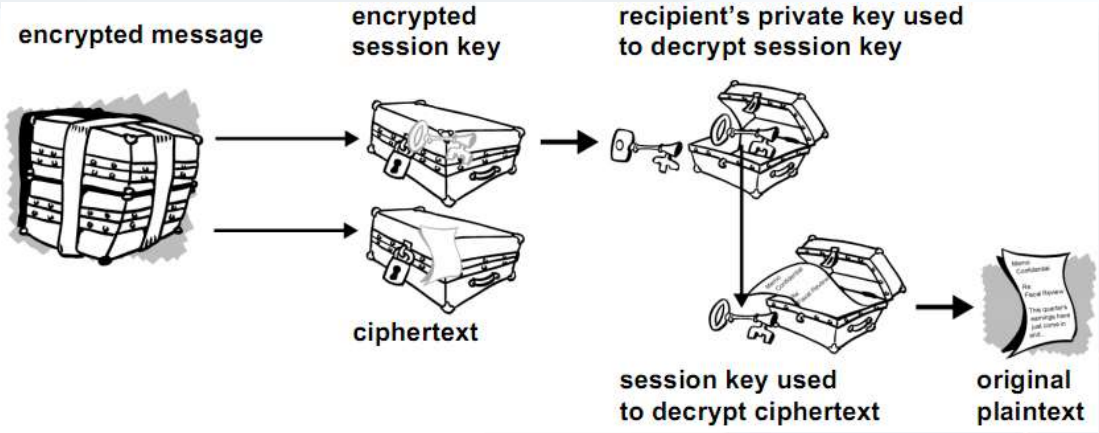
Implementasi

- Contoh Algoritma:
  - RSA, ECC
- Penggunaan:
  - Secure Socket Layer (SSL)
    - HTTPS
    - SSH
  - Pretty Good Privacy (PGP)
  - GNU Privacy Guard (GPG)

PGP (Pretty Good Privacy)

PGP
Encryption





PGP
Decryption

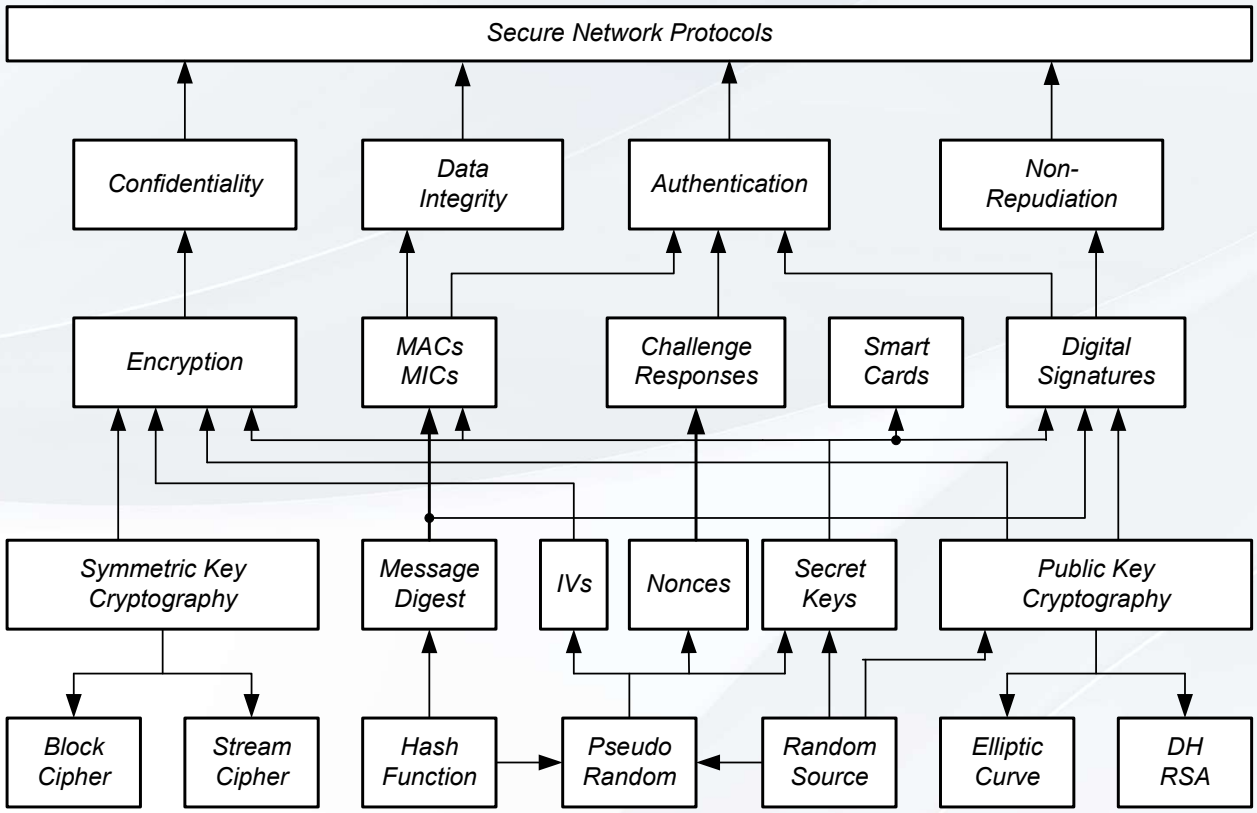
Hash Function

- Merupakan fungsi satu arah yang dapat menghasilkan ciri (signature) atau message diggest dari sebuah (data)
- Perubahan satu bit saja akan mengubah hash secara drastis
- Digunakan untuk menjamin integritas dan digital signature
- Contoh algoritma: MD5, SHA1

Penggunaan Hash

- Hasil hash dienkripsi untuk menjamin keamanannya (integritas)
- Ukuran hasil hash yang lebih kecil dibandingkan ukuran pesan asalnya membutuhkan waktu enkripsi yang lebih singkat (dibandingkan jika mengenkripsi seluruh pesan)
- Digital Signature
- Pesan juga dapat dienkripsi jika diinginkan kerahasiaan

Modern Cryptography Diagram



Question ?

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First