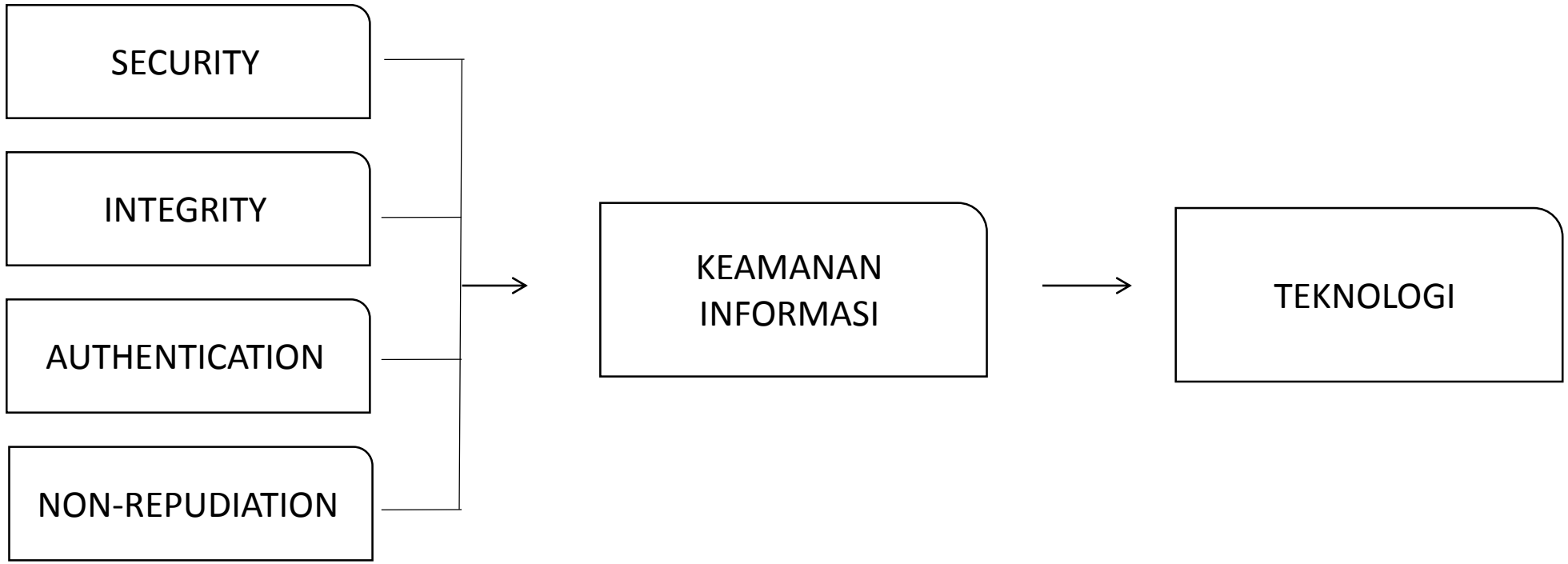
Security, Integrity, Authentication, Non-repudiation and Mathematics

Mona Elviyenti, M.Si
Jurusan Teknik Elektronika
Politeknik Caltex Riau
2017

Introduction



SECURITY

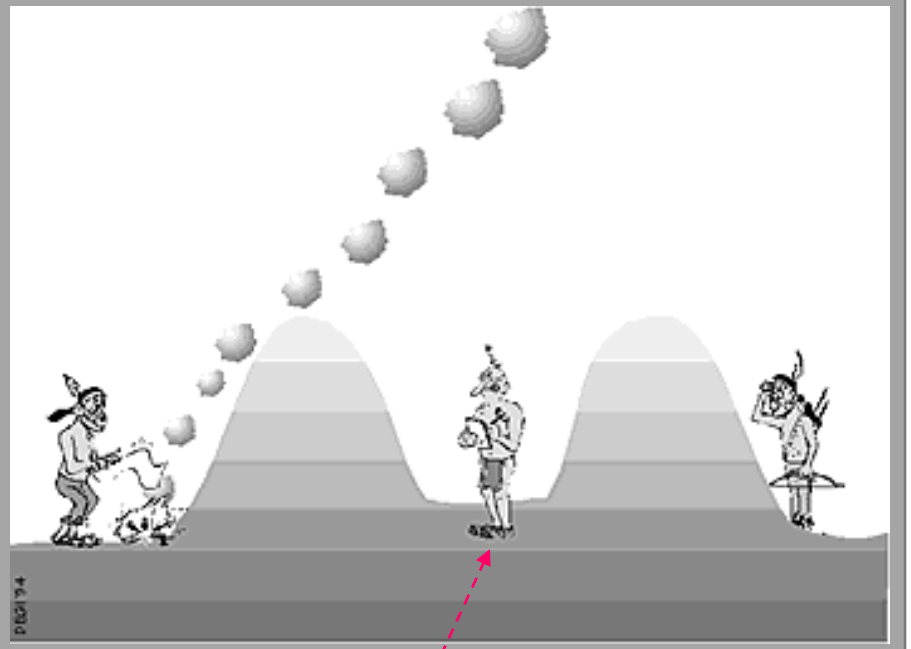
INTEGRITY

AUTHENTICATION

NON-REPUDIATION

KEAMANAN / KERAHASIAAN

Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.



Dia bisa ikut menerima pesan tapi tidak mengerti

SECURITY

INTEGRITY

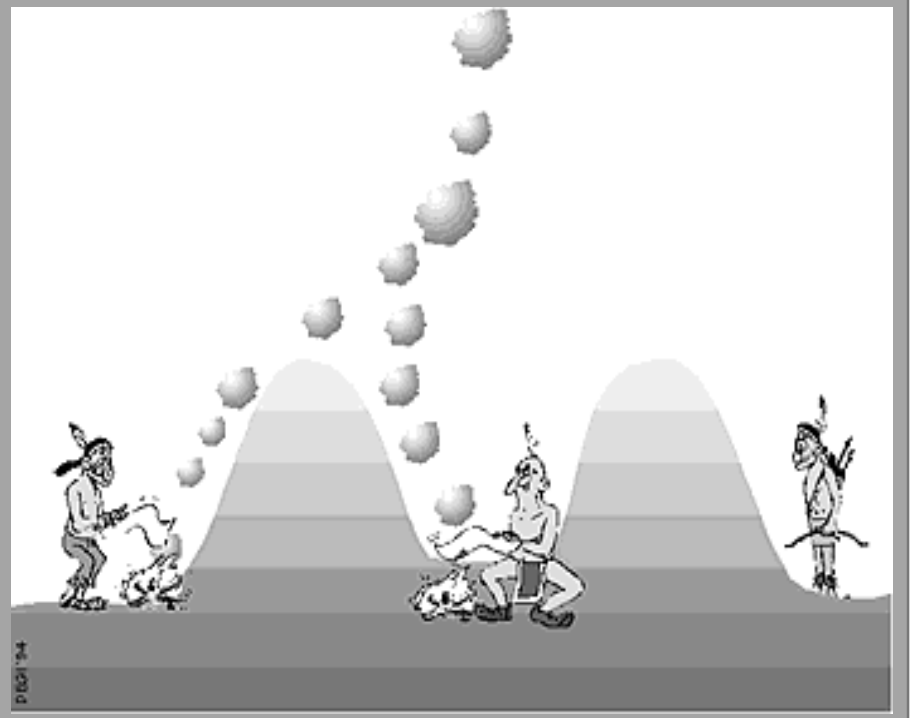
AUTHENTICATION

NON-REPUDIATION

INTEGRITAS DATA

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

“Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”.



SECURITY

INTEGRITY

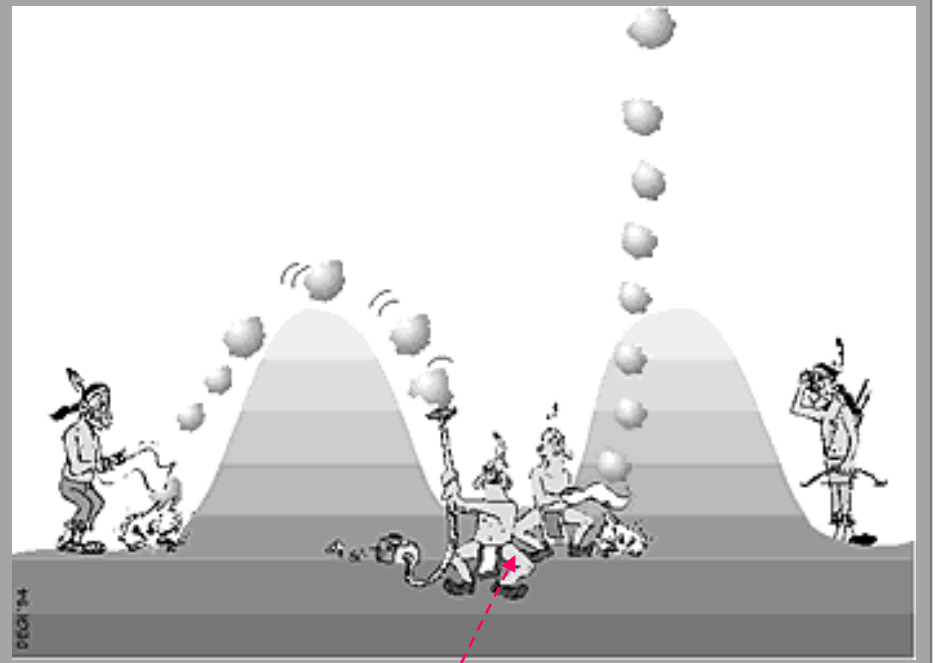
AUTHENTICATION

NON-REPUDIATION

OTENTIFIKASI

Layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi dan untuk mengidentifikasi kebenaran sumber pesan.

“Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?”



He can claim that he is A

SECURITY

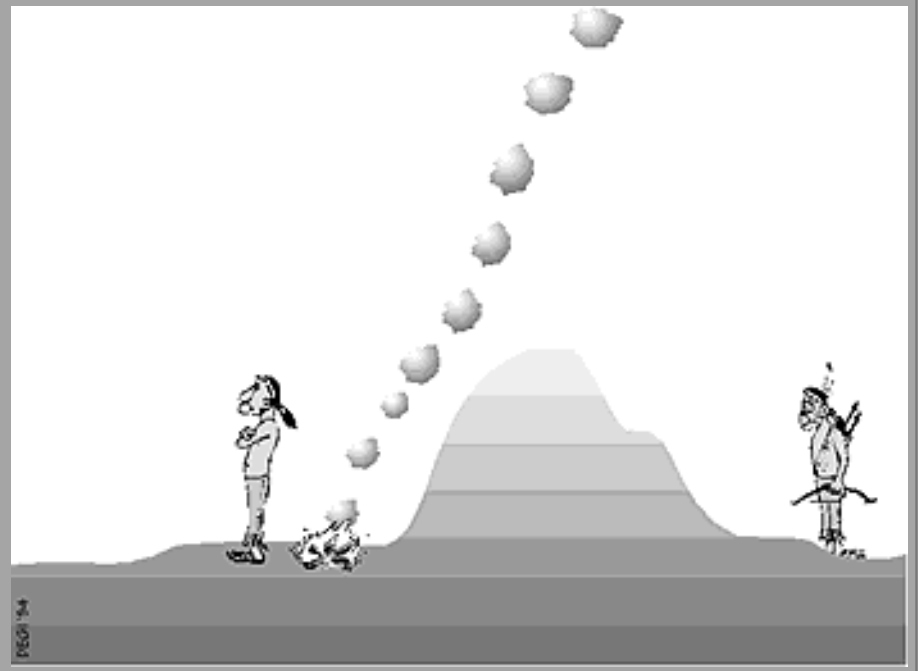
INTEGRITY

AUTHENTICATION

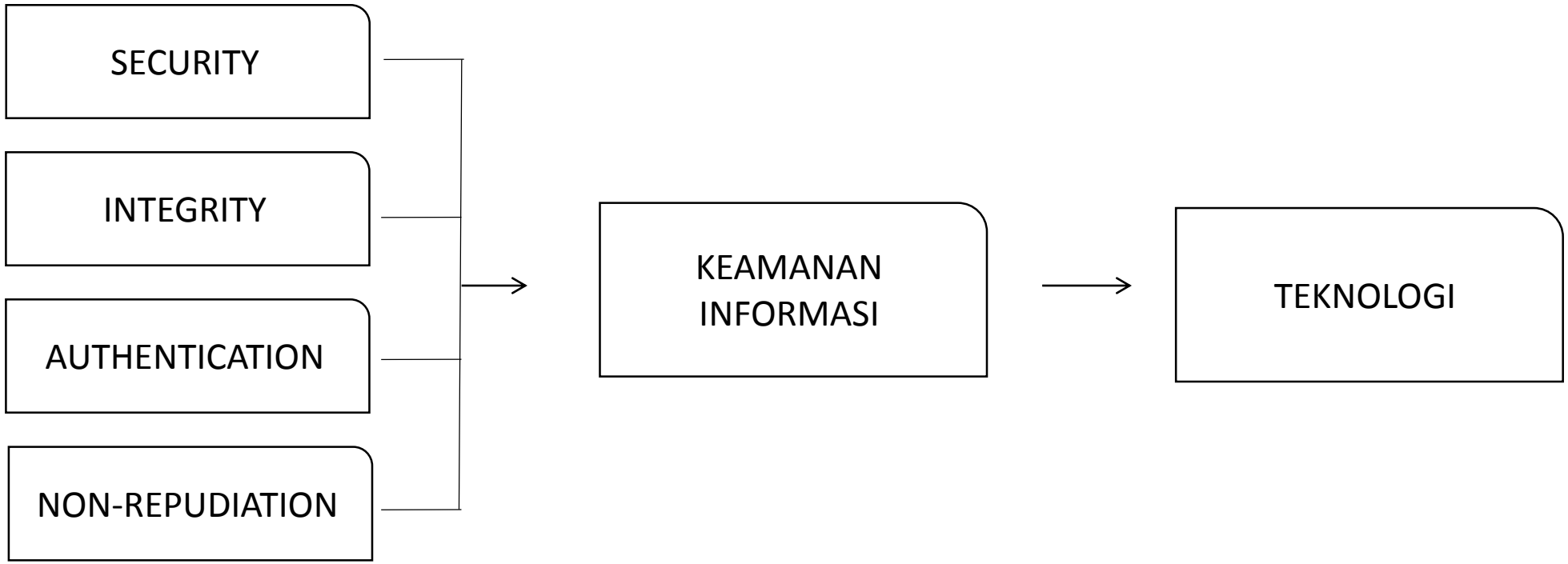
NON-REPUDIATION

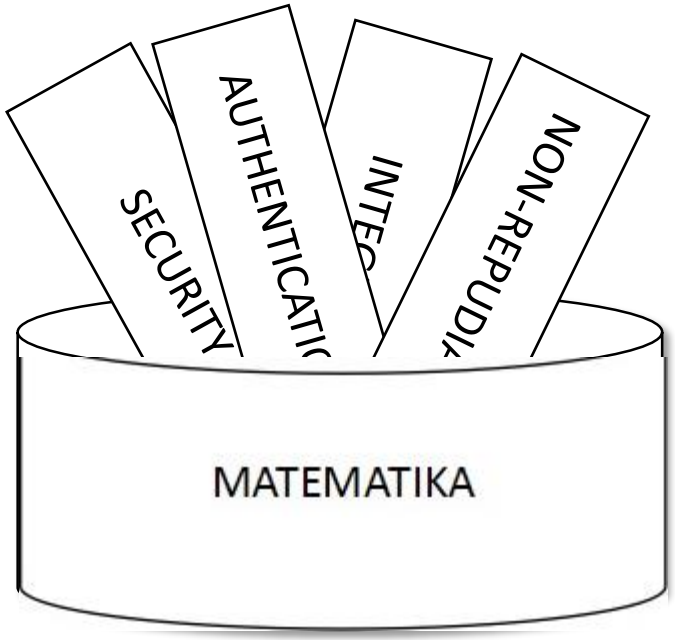
NIRPENYANGKALAN

Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.



Introduction





CRYPTOGRAPHY

⇕

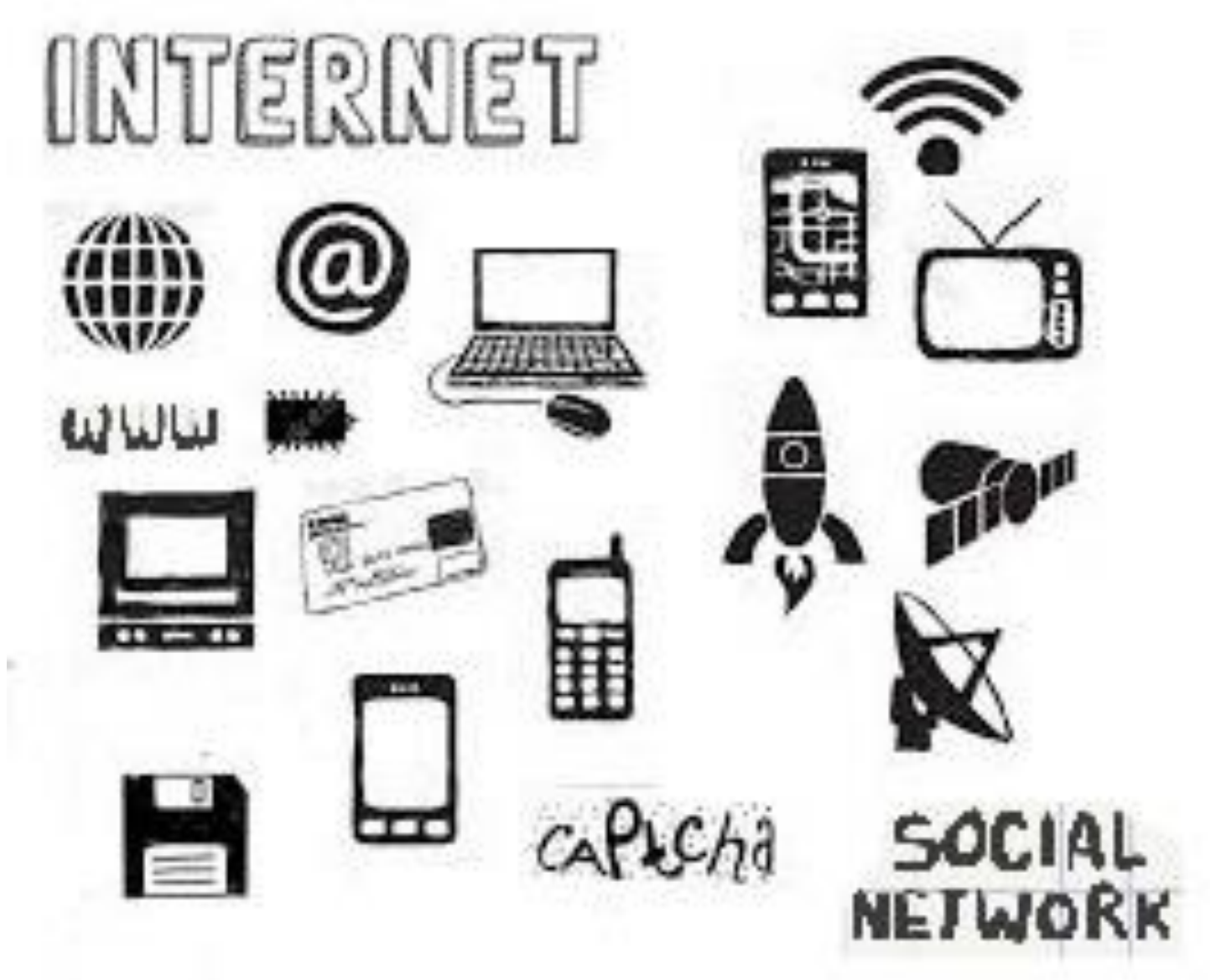
CODING THEORY

⇓

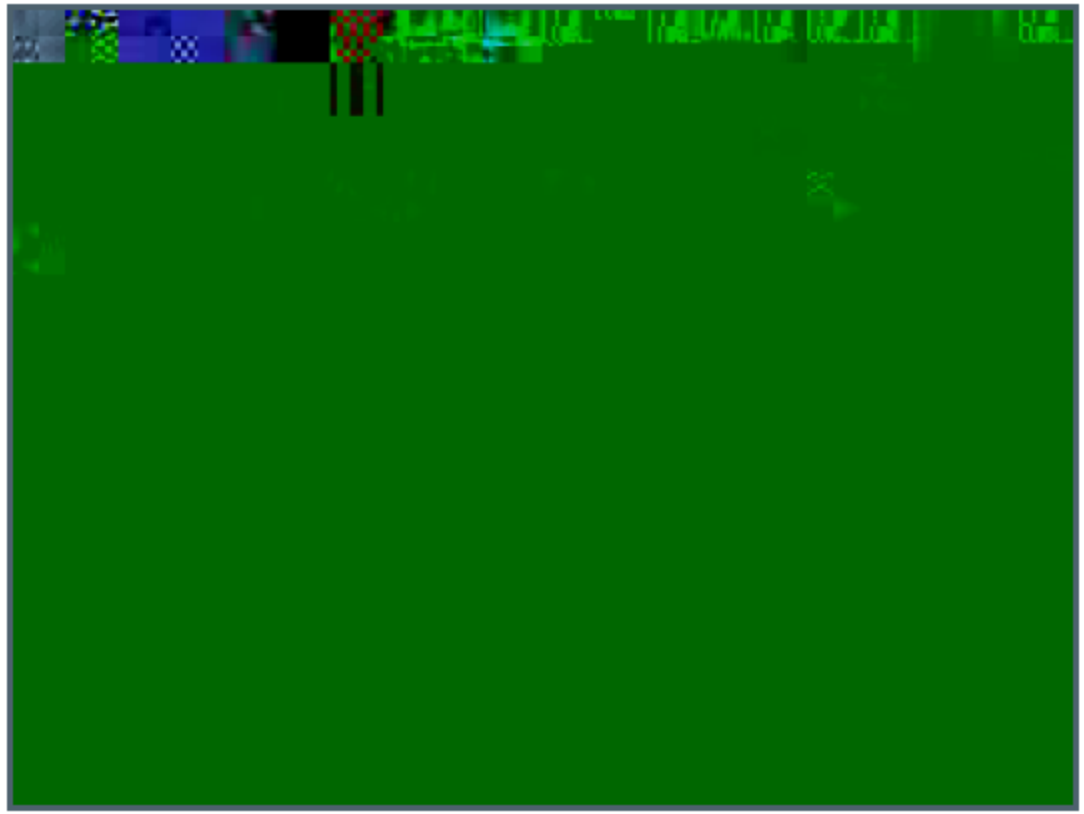
ERROR CORRECTING CODES

DATA COMPRESSION

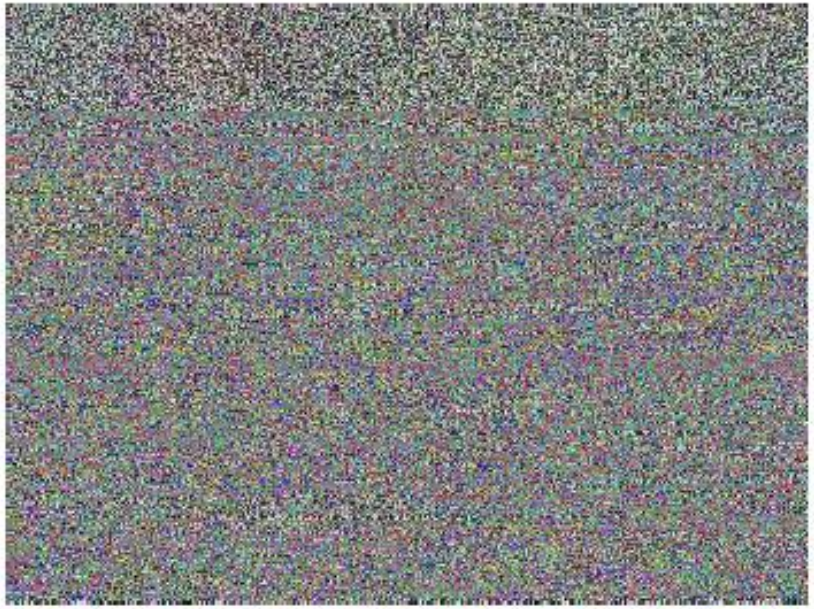
TEKNOLOGI



Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/• p}âpx;
épêp/|t}t|äzp}/qp}êpz/étzp{x/zt• xâx
}vêp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
ppsp{pw/p}pz<p}pz/zt• xâx}v/êp}
v/qpüä|t}tâpé/spüx/sp{p|/• péxü=/]
p{äüx|ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pwât• pâ/ztwxsä• p}/|tützp=



TEKS

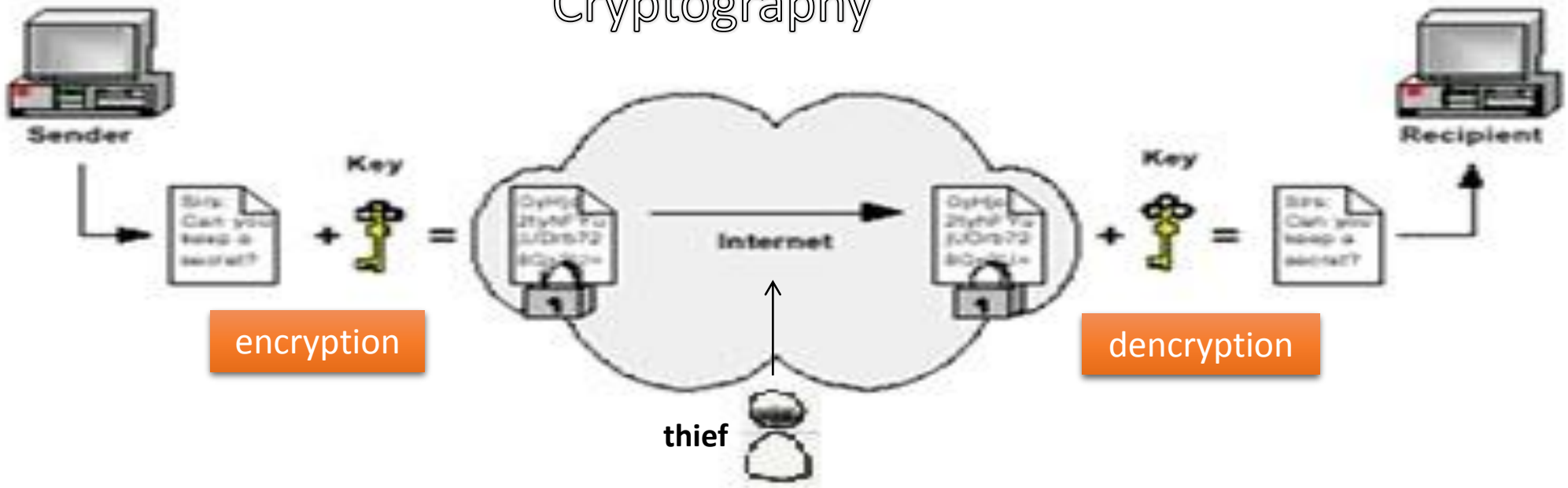


GAMBAR

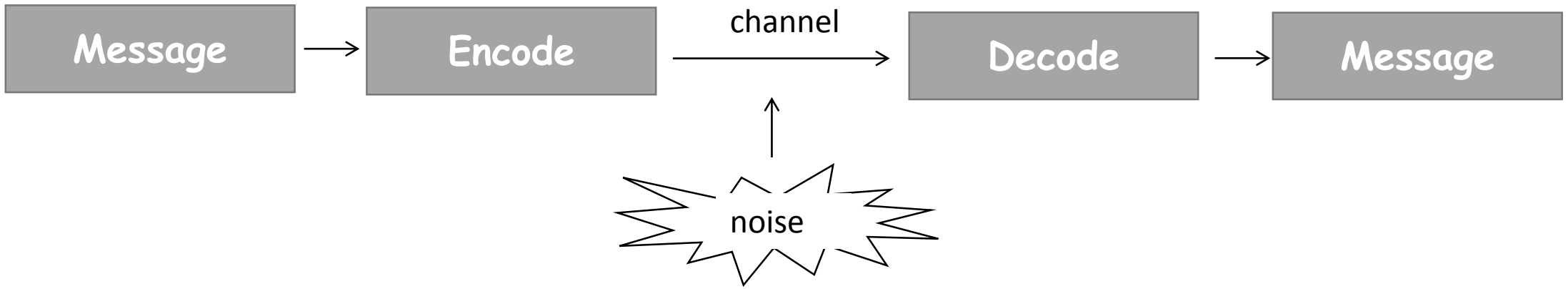
VIDEO

Ketika saya berjalan-jalan di pantai, saya menemukan banyak sekali kepiting yang merangkak menuju laut. Mereka adalah anak-anak kepiting yang baru menetas dari dalam pasir. Naluri mereka mengatakan bahwa laut adalah tempat kehidupan mereka.

Cryptography

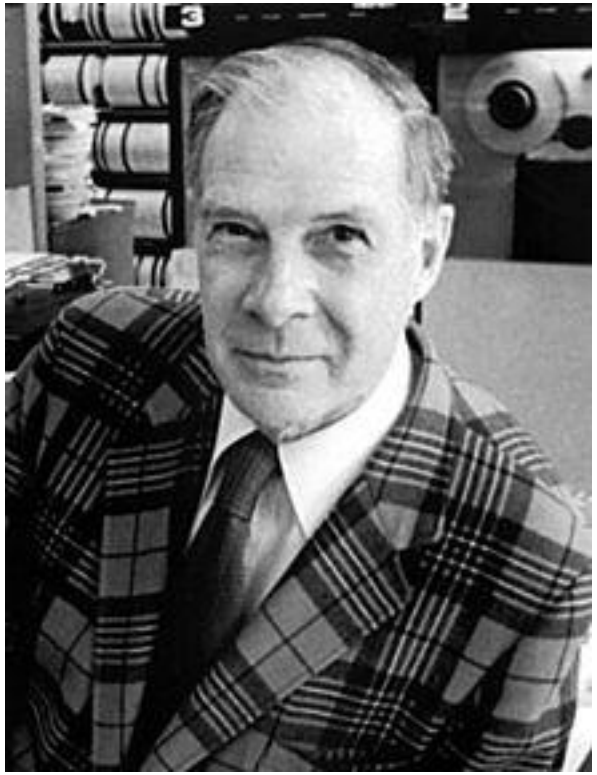


Error Correcting Codes



Claude Elwood Shanon
1916 - 2001

Dikenal sebagai The Father of Information Theory. Papernya yang berjudul Mathematical Theory of Communication (1948) menjadi cikal bakal dari ilmu Coding Theory dan Modern Cryptography.



Richard Wesley Hamming
1915 - 1998

Kontribusinya diantaranya Hamming Codes, Hamming Distance, Hamming numbers dll, memiliki impilkasi yang sangat besar pada ilmu komputer dan telekomunikasi.

THE MATHEMATICS

Diskrit

Matematika Diskrit

- Logika Matematika
- Relasi dan Fungsi
- Teori Bilangan
- Permutasi dan Kombinasi
- Dll

Aljabar

- Aljabar Linier
- Aljabar Abstrak
  - Group
  - Ring
  - Field (Galois Field)
  - Aritmatika Polinom

- ✓ Pengembangan ide dalam algoritma.
- ✓ Membuat hubungan antara kebutuhan atau keperluan dan ketentuan (aturan).
- ✓ Operasi yang mungkin untuk dilakukan.

Cryptography

>> Proses Enkripsi dan Dekripsi

Caesar Cipher, Vigenere Cipher (klasik)

$C = E(P) = (p_i + k_i) \bmod 26$

$P = D(C) = (c_i - k_i) \bmod 26$

Chiper - Feedback (modern - kunci simetri)

$C_i = E(P_i) = P_i \oplus E_k(C_{i-1})$

$P_i = D(P_i) = C_i \oplus D_k(C_{i-1})$

Chiper - Block (modern - kunci asimetri)

$C = E_e(P) \equiv p^e \pmod{n}$

$P = D_d(C) \equiv c^d \pmod{n}$

Error Correction Codes

Definition 4.2.1 A *linear code* C of length n over $\mathbf{F}_q$ is a subspace of $\mathbf{F}_q^n$.

Example 4.2.2 The following are linear codes:

(i) $C = \{(\lambda, \lambda, \ldots, \lambda) : \lambda \in \mathbf{F}_q\}$. This code is often called a *repetition code* (refer also to Example 1.0.3).
(ii) $(q = 2)\ C = \{000, 001, 010, 011\}$.
(iii) $(q = 3)\ C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$.
(iv) $(q = 2)\ C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definition 6.2.1 The (*first order*) *Reed–Muller codes* $\mathcal{R}(1, m)$ are binary codes defined, for all integers $m \geq 1$, recursively as follows:

(i) $\mathcal{R}(1, 1) = \mathbf{F}_2^2 = \{00, 01, 10, 11\}$;
(ii) for $m \geq 1$,

$$\mathcal{R}(1, m + 1) = \{(\mathbf{u}, \mathbf{u}) : \mathbf{u} \in \mathcal{R}(1, m)\} \cup \{(\mathbf{u}, \mathbf{u} + \mathbf{1}) : \mathbf{u} \in \mathcal{R}(1, m)\}.$$

Example 6.2.2 $\mathcal{R}(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$. A generator matrix of $\mathcal{R}(1, 2)$ is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Definition 4.5.1 (i) A *generator matrix* for a linear code C is a matrix G whose rows form a basis for C.

(ii) A *parity-check matrix* H for a linear code C is a generator matrix for the dual code $C^{\perp}$.

Definition 4.5.3 (i) A generator matrix of the form $(I_k|X)$ is said to be in *standard form*.

(ii) A parity-check matrix in the form $(Y|I_{n-k})$ is said to be in *standard form*.

Kriptografi klasik

Cipher Subsitusi, Cipher Transposisi, Affine Cipher, Vigenere Cipher, Playfair Cipher, Enigma Cipher, One-Time Pad

Kriptografi modern - kunci simetri

DES (Data Encryption Standard), GOST (Gosudarstvenny Standard), RC5 (oleh Ron Rivest), AES (Advanced Encryption Standard)

Kriptografi modern - kunci asimetri

RSA (Ron Rivest, Adi Shamir dan Leonard Adleman), Knapsack, Rabin, ElGamal, ECC (Elliptic Curve Cryptography)

TERIMA KASIH