KRIPTOGRAFI DAN STEGANOGRAFI

Program Studi Informatika

Sesi 5 – Kriptografi Asymmetric

Abdul Azzam Ajhari, S.Kom., M.Kom.

Refreshment Sesi 4

Blok Cipher

Dalam blok cipher, algoritma Cipher bekerja pada blok data dengan ukuran tetap. Misalnya, jika ukuran blok delapan, delapan byte plaintext dienkripsi sekaligus.

Biasanya, antarmuka pengguna untuk operasi enkripsi/dekripsi menangani data yang lebih panjang dari ukuran blok dengan berulang kali memanggil fungsi sandi tingkat rendah.

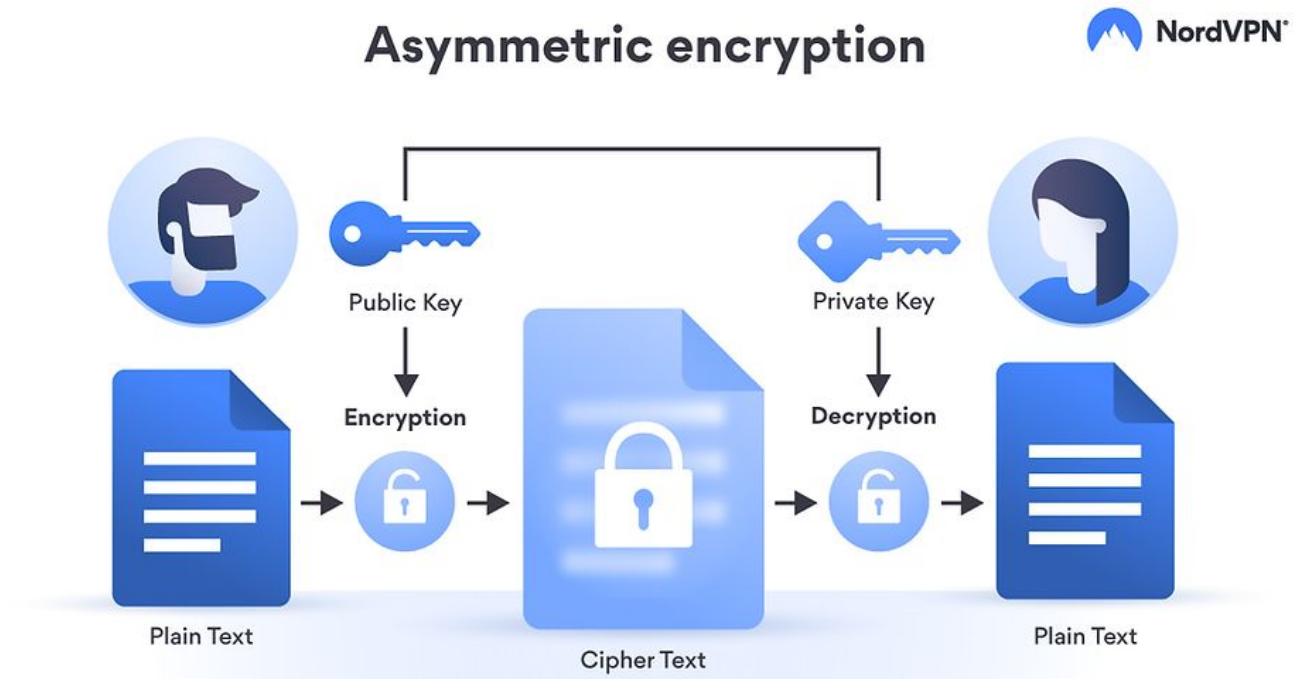
Stream Cipher

Stream cipher tidak bekerja berdasarkan blok, melainkan mengonversi satu bit (atau satu byte) data pada satu waktu.

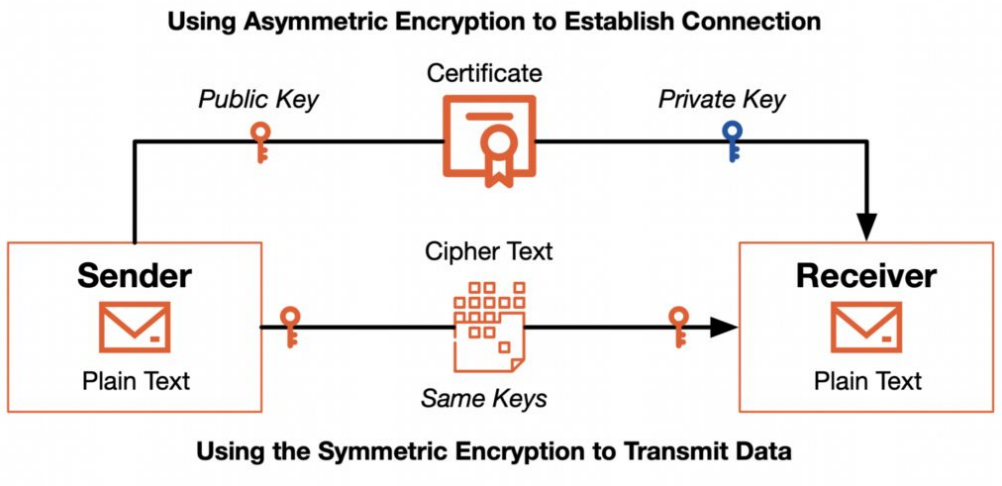
Pada dasarnya, stream cipher menghasilkan keystream berdasarkan kunci yang disediakan. Keystream yang dihasilkan kemudian di-XOR dengan data plaintext.

Kriptografi Asymmetric

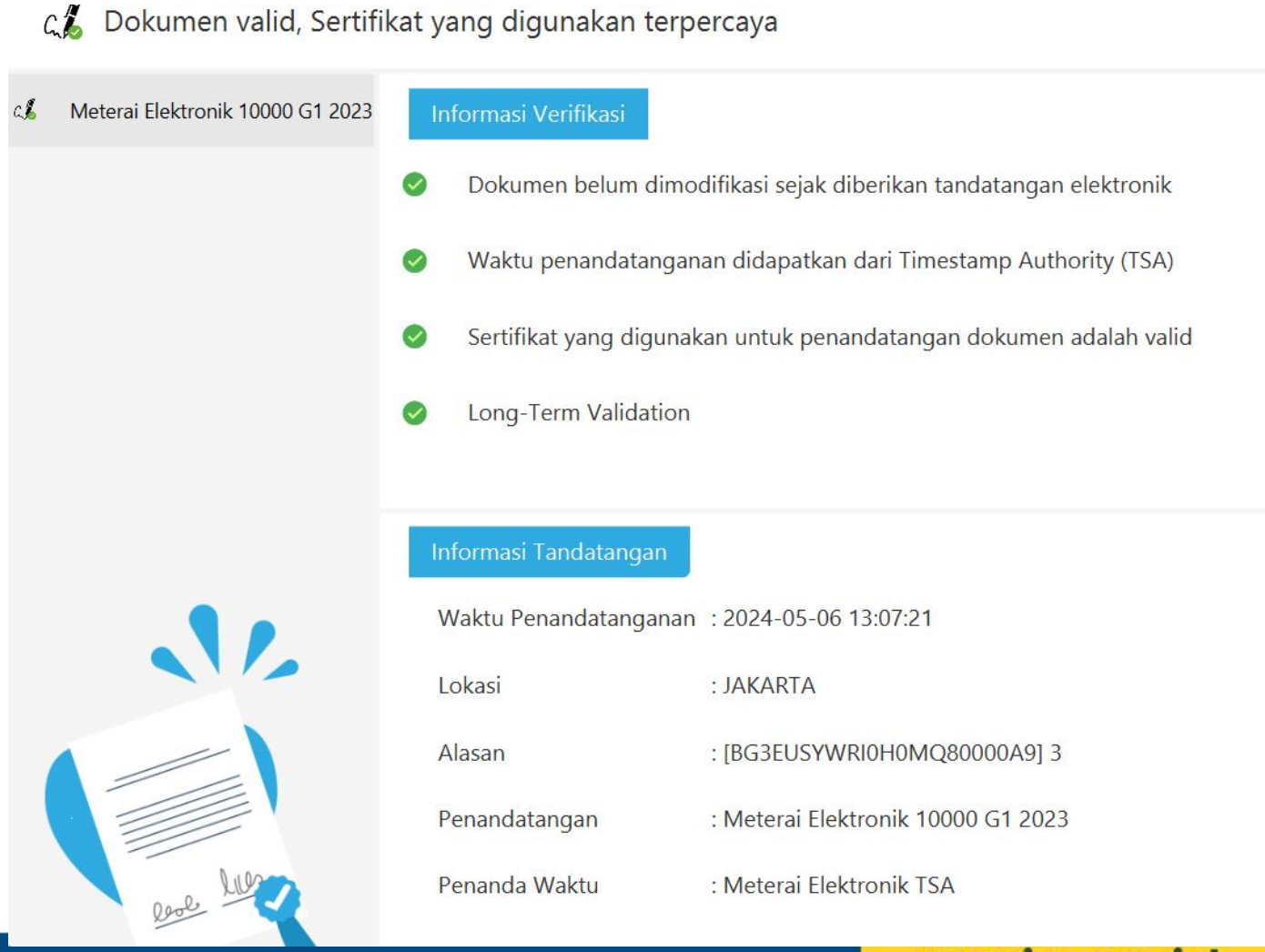
Kriptografi asimetris juga disebut sebagai kriptografi kunci publik. Ini adalah metode kriptografi paling populer yang digunakan untuk mengenkripsi dan mendekripsi pesan untuk menyediakan keamanan data di sebagian besar jaringan komunikasi. Sepasang kunci yang berbeda digunakan: kunci publik dan kunci privat.

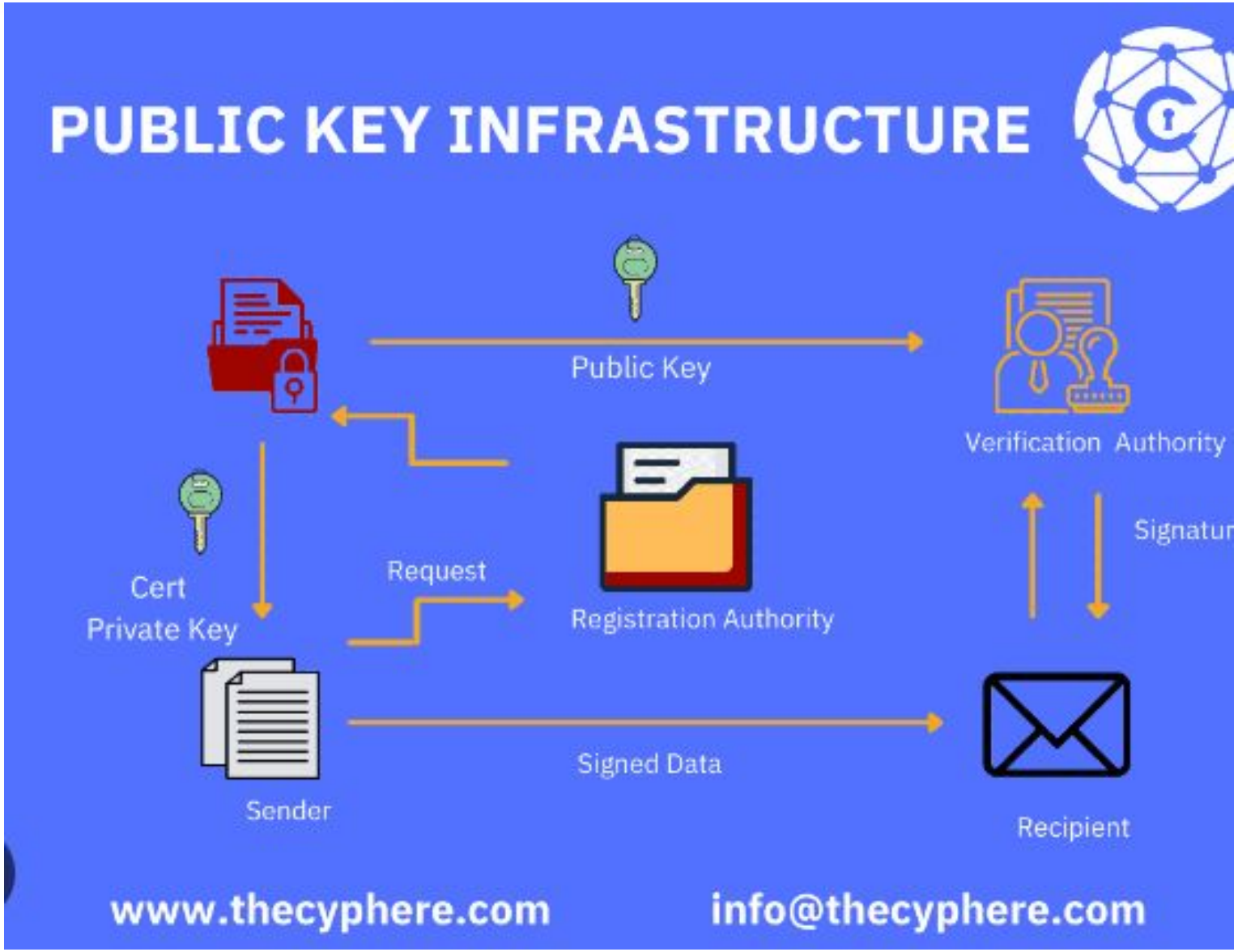


Kriptografi Asymmetric in Daily Life

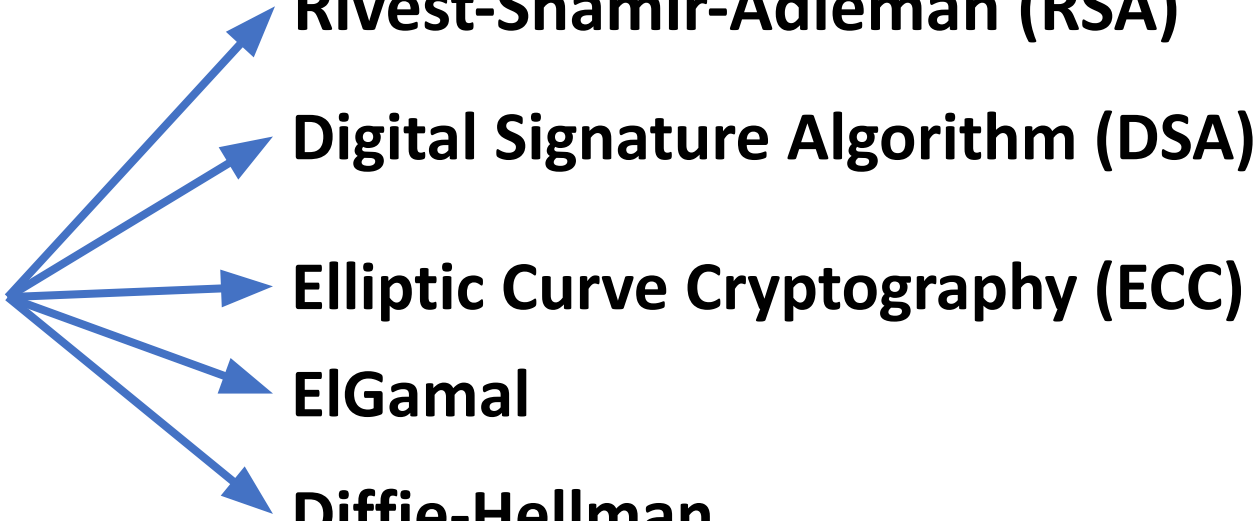


Sumber gambar: Tetrate




PUBLIC KEY INFRASTRUCTURE
Public Key
Verification Authority
Signatur
Request
Cert
Private Key
Registration Authority
Signed Data
Sender
Recipient
www.thecyphere.com
info@thecyphere.com

Algoritma Kriptografi Asymmetric (Commonly Used)



Contoh Penerapan Algoritma Rivest-Shamir-Adleman (RSA)

Rivest-Shamir-Adleman (RSA)

Diketahui

- Plainteks = ‘Saya adalah mahasiswa UNSIA’
- P = 61
- Q = 53
- e = 17 (kunci public)
- d = 2753 (kunci privat)

Rivest-Shamir-Adleman (RSA)

Hitung nilai modulus n

$n = P \times Q$

$= 61 \times 53 = 3233$

Hitung Nilai Totient $\phi(n)$

$\varphi(n) = (P-1) \times (Q-1)$

$= 60 \times 52 = 3120$

Rivest-Shamir-Adleman (RSA)

Konversi ke bentuk numerik (ASCII)

Karakter	ASCII
S	83
a	97
y	121
a	97
(spasi)	32

Rivest-Shamir-Adleman (RSA)

Konversi ke bentuk numerik (ASCII)

a	97
d	100
a	97
l	108
a	97
h	104
(spasi)	32

Rivest-Shamir-Adleman (RSA)

Konversi ke bentuk numerik (ASCII)

m	109
a	97
h	104
a	97
s	115
i	105
w	119
a	97
(spasi)	32

Rivest-Shamir-Adleman (RSA)

Konversi ke bentuk numerik (ASCII)

U	85
N	78
S	83
I	73
A	65

Rivest-Shamir-Adleman (RSA)

- Enkripsi menggunakan kunci public e=17 dan n=3233

$$C = M^e \ mod \ n$$

Dimana:

- C adalah cipher (hasil enkripsi),
- M adalah pesan dalam bentuk numerik (nilai ASCII),
- e adalah kunci publik, dan
- n adalah modulus.

Rivest-Shamir-Adleman (RSA)

Enkripsi kata pertama ‘S’ (ASCII = 83)

$$C = 83^{17}\ mod\ 3233$$

Pertama, kita hitung 83^{17} secara bertahap. Gunakan eksponen bertingkat untuk mempermudah perhitungan

1. $83^2 \mod 3233$:

$$83^2 = 6889, \quad 6889 \mod 3233 = 423$$

2. $83^4 \mod 3233$:

$$(423)^2 = 178929, \quad 178929 \mod 3233 = 1114$$

3. $83^8 \mod 3233$:

$$(1114)^2 = 1240996, \quad 1240996 \mod 3233 = 645$$

4. $83^{16} \mod 3233$:

$$(645)^2 = 416025, \quad 416025 \mod 3233 = 2201$$

5. $83^{17} \mod 3233$:

$$83^{17} = 83^{16} \cdot 83, \quad 2201 \cdot 83 = 182683, \quad 182683 \mod 3233 = 2595$$

Jadi, hasil enkripsi untuk 'S' adalah **2595**.

Rivest-Shamir-Adleman (RSA)

Lakukan langkah yang sama untuk setiap karakter pesan

Karakter	ASCII	Enkripsi (C = M^17 mod 3233)
S	83	2595
a	97	1322
y	121	1521
a	97	1322
(spasi)	32	2483

Rivest-Shamir-Adleman (RSA)

Lakukan langkah yang sama untuk setiap karakter pesan

a	97	1322
d	100	1264
a	97	1322
l	108	2749
a	97	1322
h	104	2449
(spasi)	32	2483

Rivest-Shamir-Adleman (RSA)

Lakukan langkah yang sama untuk setiap karakter pesan

m	109	1061
a	97	1322
h	104	2449
a	97	1322
s	115	518
i	105	951
w	119	876
a	97	1322
(spasi)	32	2483

Rivest-Shamir-Adleman (RSA)

Lakukan langkah yang sama untuk setiap karakter pesan

U	85	2621
N	78	2449
S	83	2595
I	73	2577
A	65	347

Rivest-Shamir-Adleman (RSA)

- Dekripsi Menggunakan Kunci Privat d=2753 dan n=3233

$$M = C^d \, mod \, n$$

Dimana:

- M adalah pesan asli yang telah didekripsi,
- C adalah cipher yang telah dienkripsi,
- d adalah kunci privat, dan
- n adalah modulus.

Rivest-Shamir-Adleman (RSA)

Dekripsi Karakter Pertama: 2595

$$M = 2595^{2753}\ mod\ 3233$$

- Lakukan perhitungan secara bertahap menggunakan metode eksponen bertingkat. Sebagai contoh, kita dapat menghitung $2595^{2753}\ mod\ 3233$ dan mendapatkan hasilnya, yang akan menghasilkan nilai ASCII yang kembali menjadi 'S'.
- Proses dekripsi untuk karakter lainnya dapat dilakukan dengan cara yang sama.
- Setelah mendekripsi semua cipher, kita mendapatkan kembali pesan asli: **"Saya adalah mahasiswa UNSIA"**.

Kekuatan Kriptografi Asimetris

1. Keamanan tingkat tinggi.
2. Tidak Perlu Bertukar *secret key*.
3. Skalabilitas tinggi.

Kelemahan Kriptografi Asimetris

1. Kecepatan lambat.
2. Membutuhkan daya komputasi tinggi.
3. Ukuran kunci besar.
4. Ketergantungan pada Public Key Infrastructure (PKI).

- Computer Security Principles and Practice Third Edition, William Stallings and Lawrie Brown, Pearson, 2012
- Introduction to computer security, Matt Bishop, Addison Wesley, 2005
- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross, and Addison-Wesley
- https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data
- https://selembardigital.com/pelajari-semua-tentang-cryptocurrency-kriptografi-bagaimana-cara-kerjanya/
- https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic-hash-functions
- Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.
- National Institute of Standards and Technology (NIST) - Publications on Secure Hash Standards (SHS)