CRYPTOGRAPHY AND STEGANOGRAPHY

Department of Informatics

Sesi 5 – Asymmetric Cryptography

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

Refreshment Sesi 4

Block Cipher

In block cipher, the Cipher algorithm works on blocks of data of fixed size. For example, if the block size is eight, eight bytes of plaintext are encrypted at a time.

Typically, the user interface for encryption/decryption operations handles data longer than the block size by repeatedly calling low-level cipher functions.

https://www.ibm.com/id-id/think/topics/cryptography-types

Stream Cipher

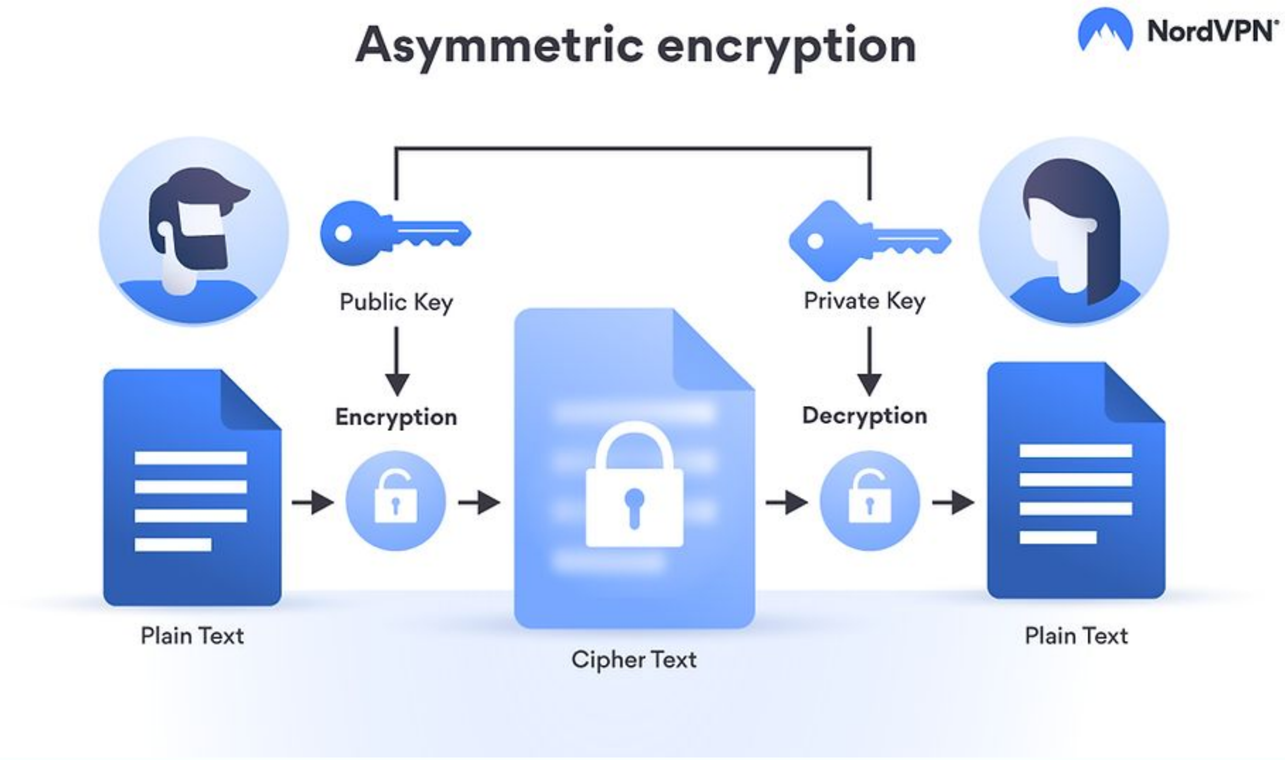
Stream ciphers do not work on a block basis, but instead convert one bit (or one byte) of data at a time.

Basically, a stream cipher generates a keystream based on a provided key. The resulting keystream is then XOR with the plaintext data.

https://www.ibm.com/id-id/think/topics/cryptography-types

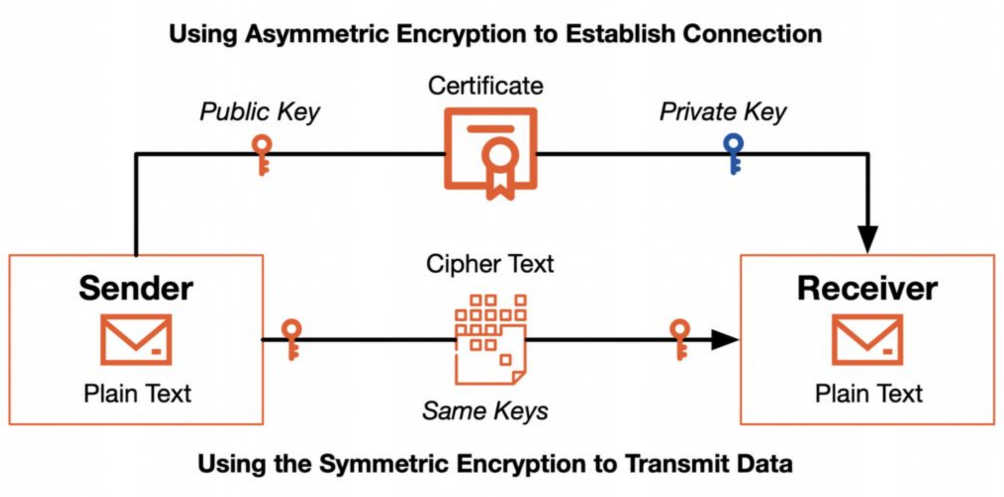
Asymmetric Cryptography

Asymmetric cryptography is also called public key cryptography. It is the most popular cryptographic method used to encrypt and decrypt messages to provide data security in most communication networks. A pair of different keys are used: a public key and a private key.



https://www.sciencedirect.com/topics/computer-science/asymmetric-cryptography

Asymmetric Cryptography in Daily Life



Using Asymmetric Encryption to Establish Connection

Public Key

Certificate

Private Key

Sender

Plain Text

Cipher Text

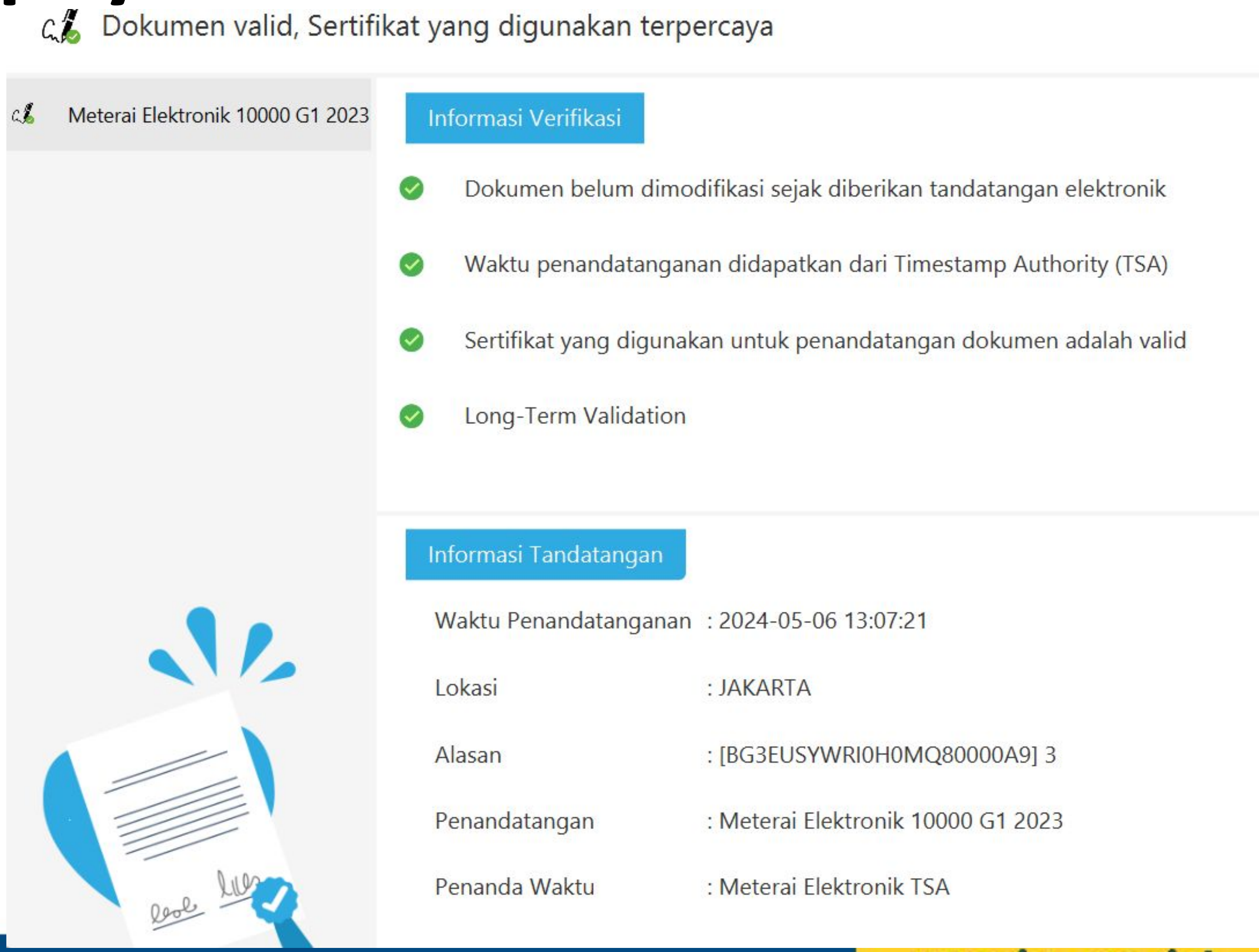
Same Keys

Receiver

Plain Text

Using the Symmetric Encryption to Transmit Data

Sumber gambar: Tetrate



Dokumen valid, Sertifikat yang digunakan terpercaya

Meterai Elektronik 10000 G1 2023

Informasi Verifikasi

- Dokumen belum dimodifikasi sejak diberikan tandatangan elektronik
- Waktu penandatanganan didapatkan dari Timestamp Authority (TSA)
- Sertifikat yang digunakan untuk penandatangan dokumen adalah valid
- Long-Term Validation

Informasi Tandatangan

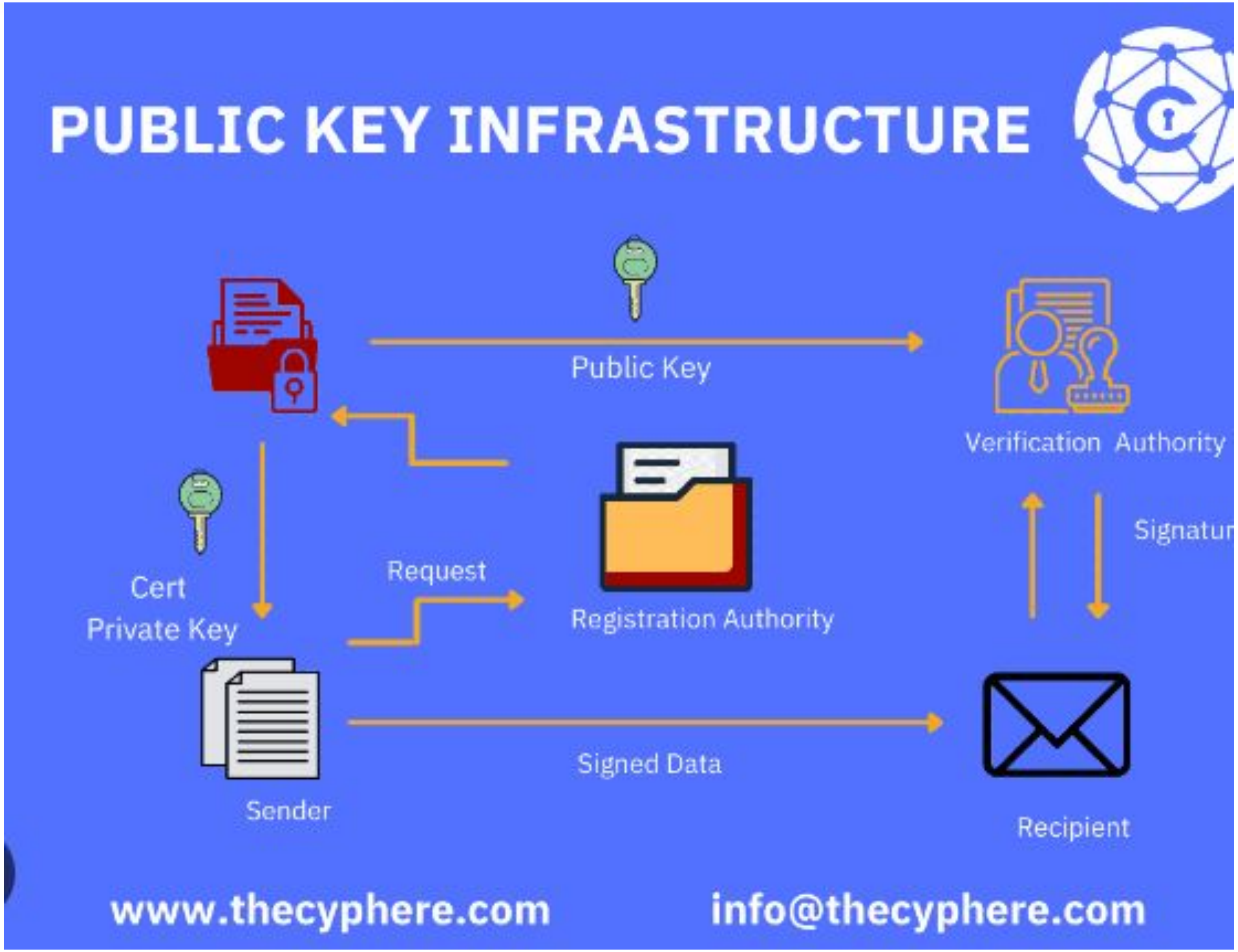
Waktu Penandatanganan : 2024-05-06 13:07:21

Lokasi : JAKARTA

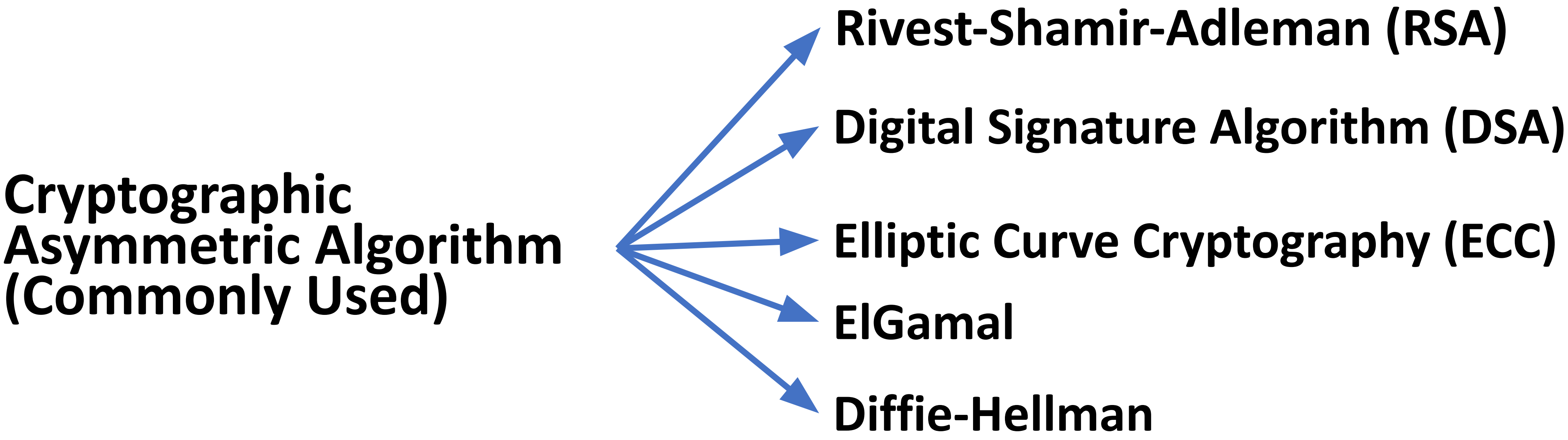
Alasan : [BG3EUSYWRI0H0MQ80000A9] 3

Penandatangan : Meterai Elektronik 10000 G1 2023

Penanda Waktu : Meterai Elektronik TSA



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



Cryptographic Asymmetric Algorithm (Commonly Used)

Rivest-Shamir-Adleman (RSA)

Digital Signature Algorithm (DSA)

Elliptic Curve Cryptography (ECC)

ElGamal

Diffie-Hellman

Example of Application of Rivest-Shamir-Adleman (RSA) Algorithm

Rivest-Shamir-Adleman (RSA)

Known

- Plaintext = ‘Saya adalah mahasiswa UNSIA’
- P = 61
- Q = 53
- e = 17 (public key)
- d = 2753 (private key)

Rivest-Shamir-Adleman (RSA)

Calculate the modulus value of n

n = P x Q

= 61 x 53 = 3233

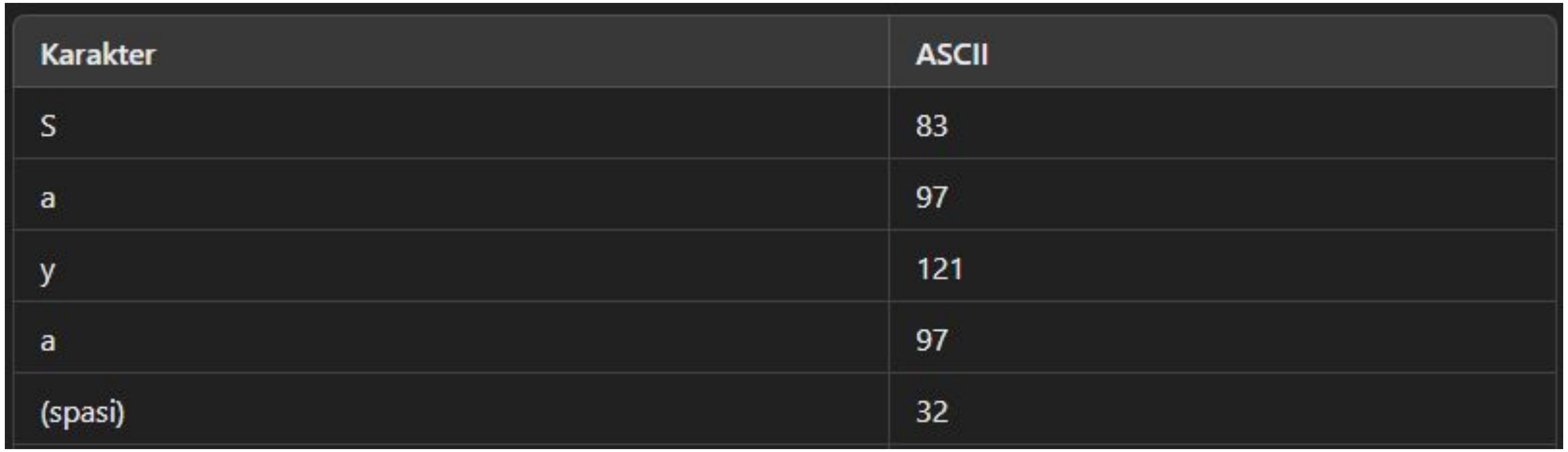
Calculate the Totient ϕ(n) Value

φ(n) = (P-1) x (Q-1)

= 60 x 52 = 3120

Rivest-Shamir-Adleman (RSA)

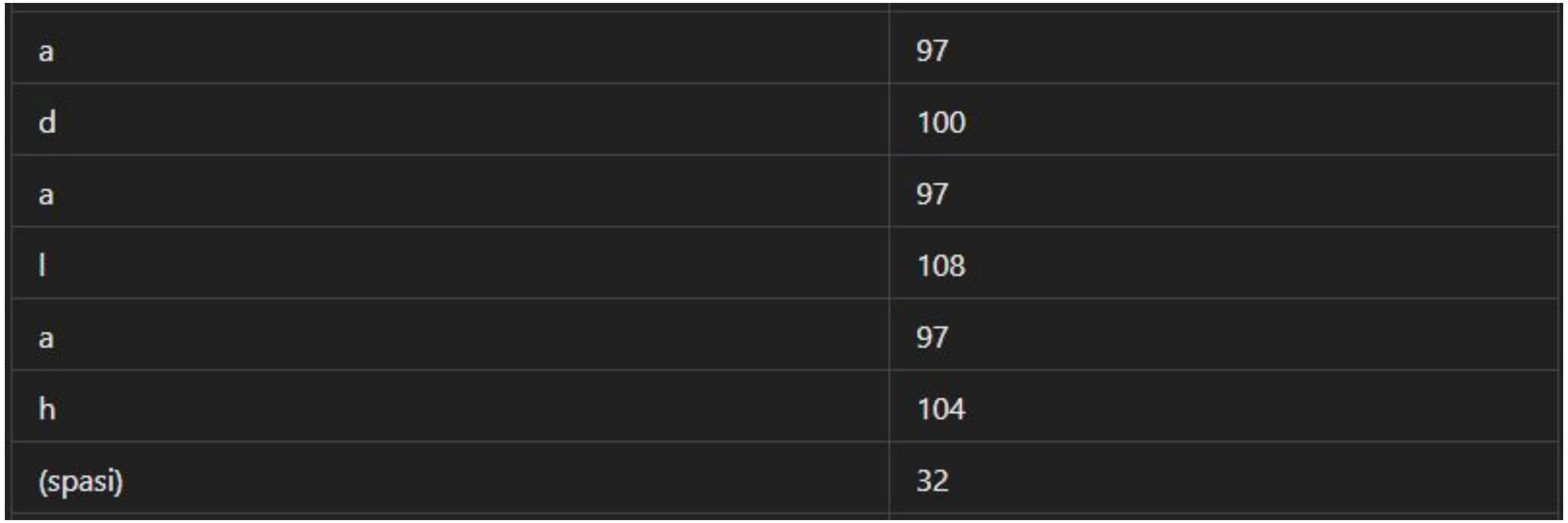
Convert to numeric form (ASCII)



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

Rivest-Shamir-Adleman (RSA)

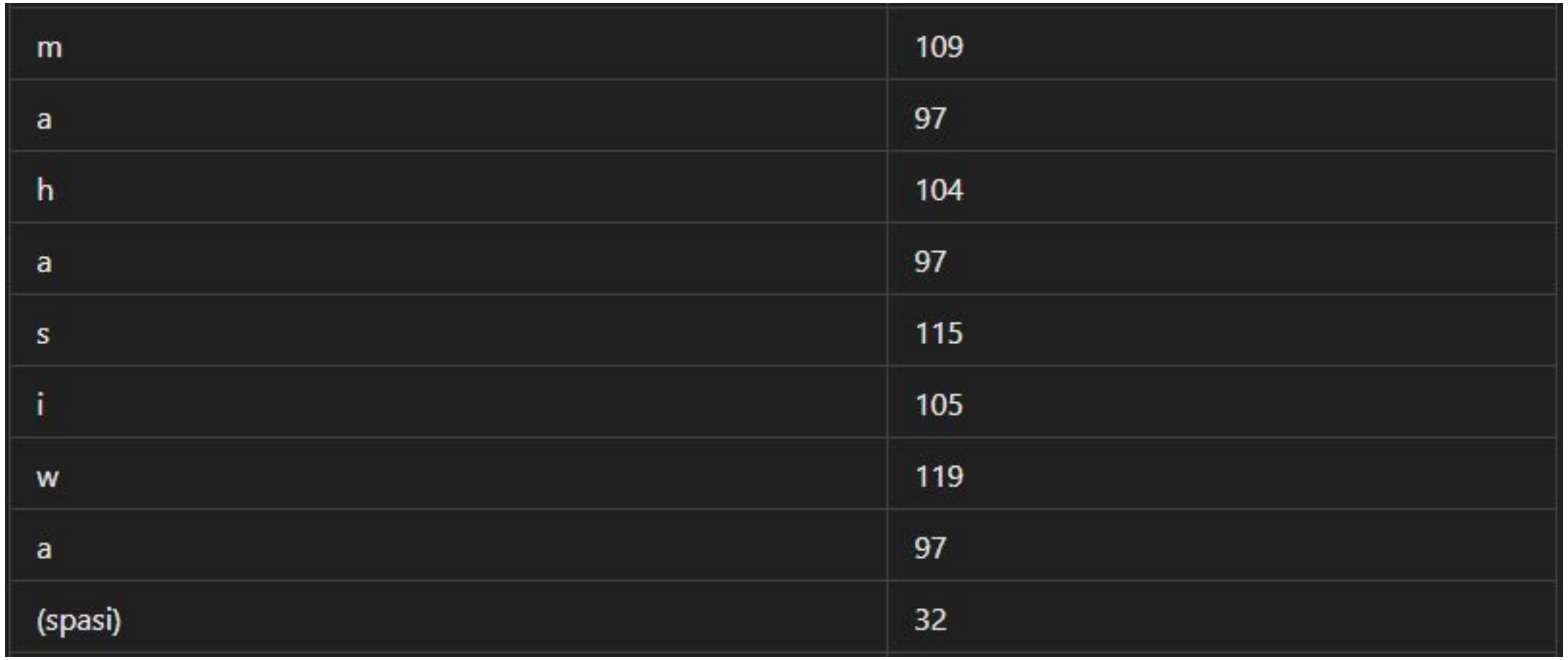
Convert to numeric form (ASCII)



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

Rivest-Shamir-Adleman (RSA)

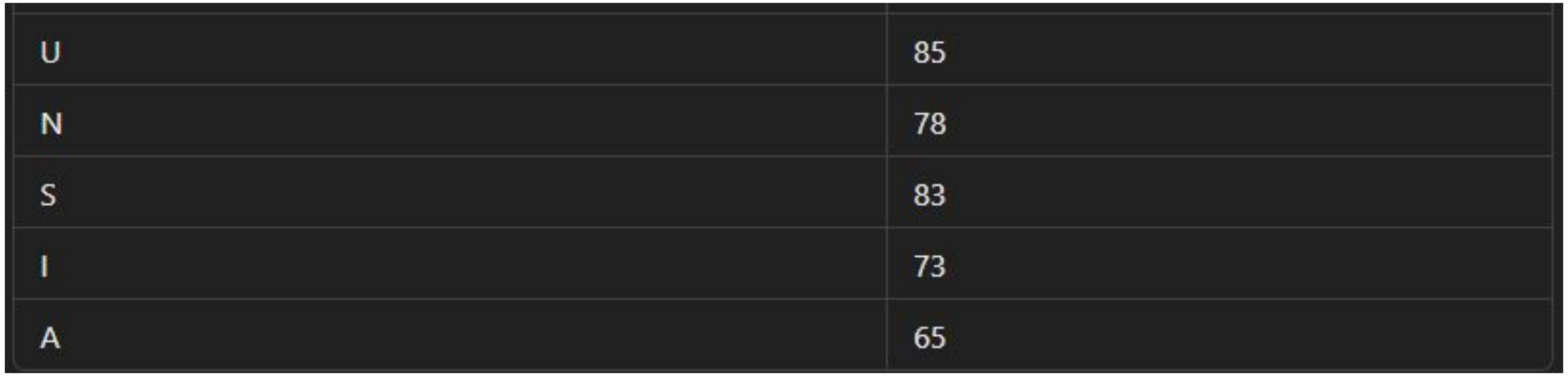
Convert to numeric form (ASCII)



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

Rivest-Shamir-Adleman (RSA)

Convert to numeric form (ASCII)



U	85
N	78
S	83
I	73
A	65

Rivest-Shamir-Adleman (RSA)

- Encryption using public key e=17 and n=3233

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

Where:

- C is cipher (encryption result),
- M is message in numeric form (ASCII value),
- e is public key
- n is modulus.

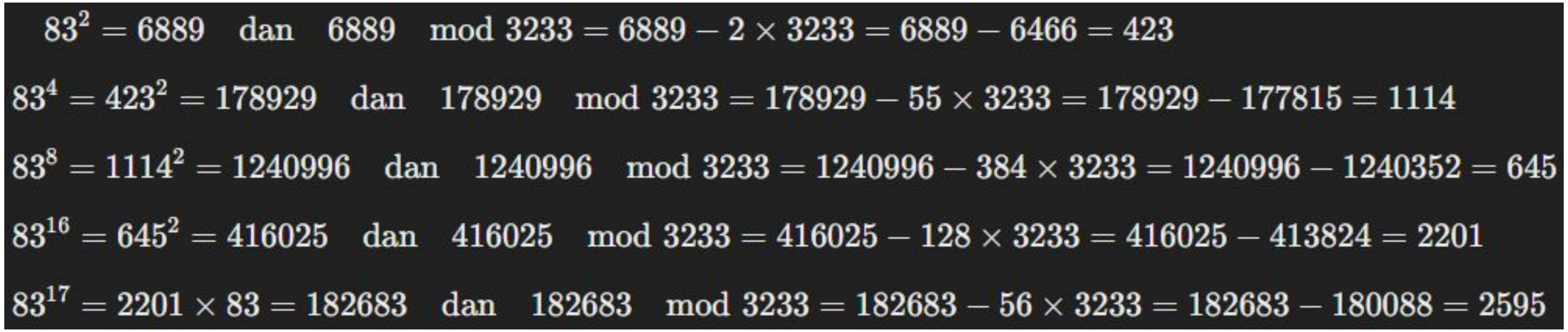
Rivest-Shamir-Adleman (RSA)

- First word encryption ‘S’ (ASCII = 83)

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

First, we calculate 83^{17} gradually.

Use nested exponents to simplify calculations.



$$83^2 = 6889 \quad \text{dan} \quad 6889 \mod 3233 = 6889 - 2 \times 3233 = 6889 - 6466 = 423$$

$$83^4 = 423^2 = 178929 \quad \text{dan} \quad 178929 \mod 3233 = 178929 - 55 \times 3233 = 178929 - 177815 = 1114$$

$$83^8 = 1114^2 = 1240996 \quad \text{dan} \quad 1240996 \mod 3233 = 1240996 - 384 \times 3233 = 1240996 - 1240352 = 645$$

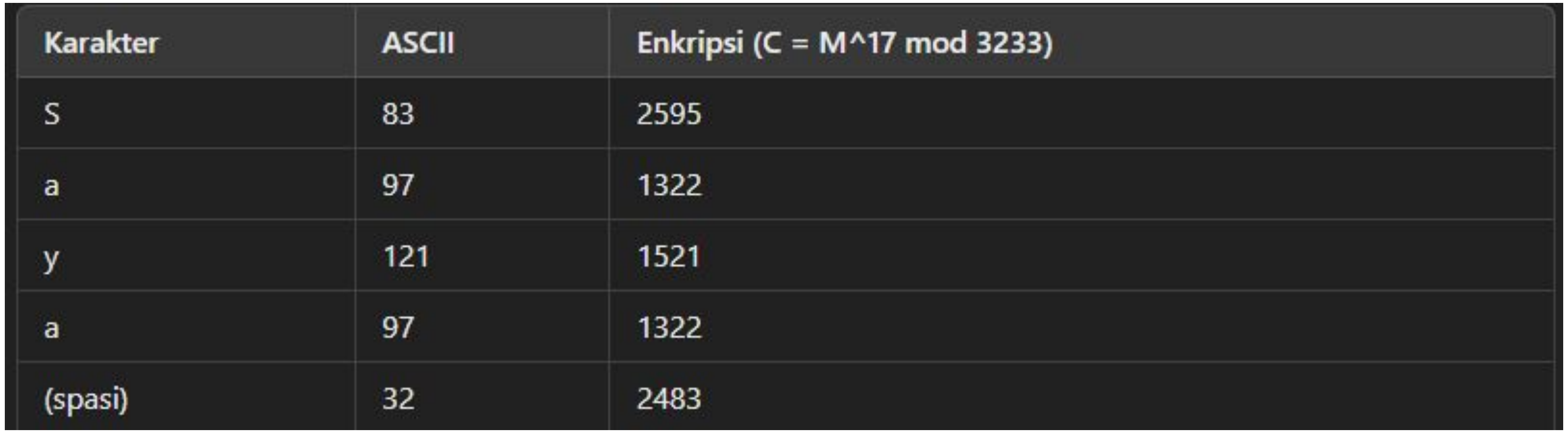
$$83^{16} = 645^2 = 416025 \quad \text{dan} \quad 416025 \mod 3233 = 416025 - 128 \times 3233 = 416025 - 413824 = 2201$$

$$83^{17} = 2201 \times 83 = 182683 \quad \text{dan} \quad 182683 \mod 3233 = 182683 - 56 \times 3233 = 182683 - 180088 = 2595$$

So, encryption results for 'S’ is **2595**.

Rivest-Shamir-Adleman (RSA)

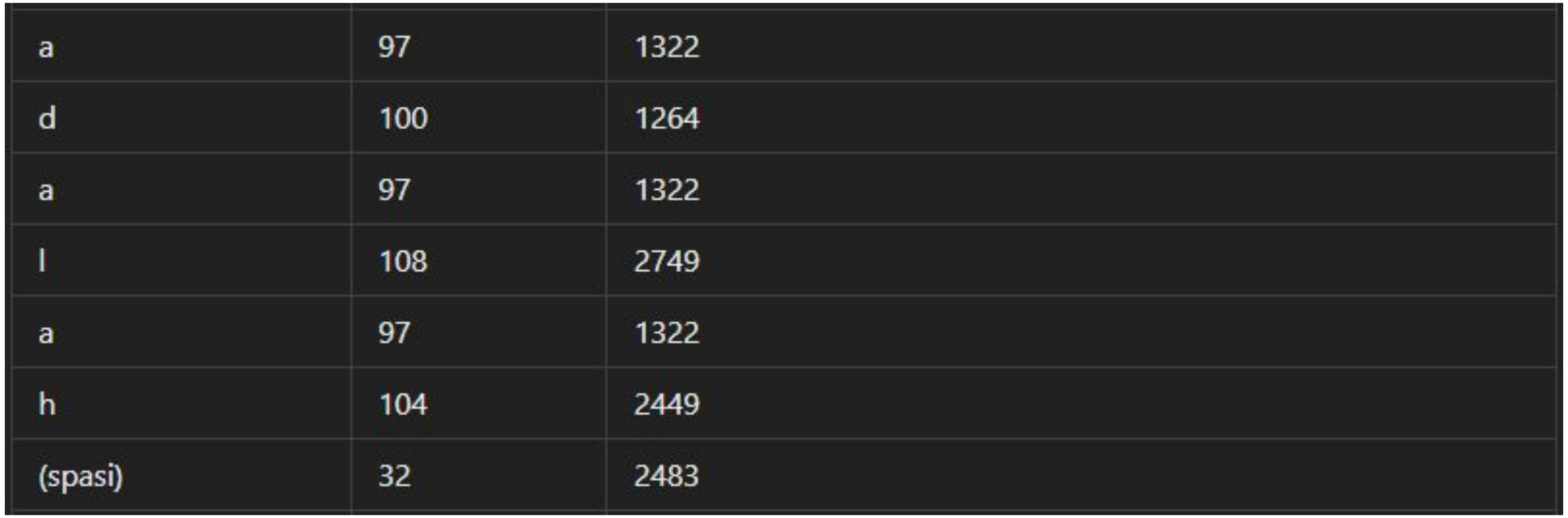
Do the same steps for each message character.



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)

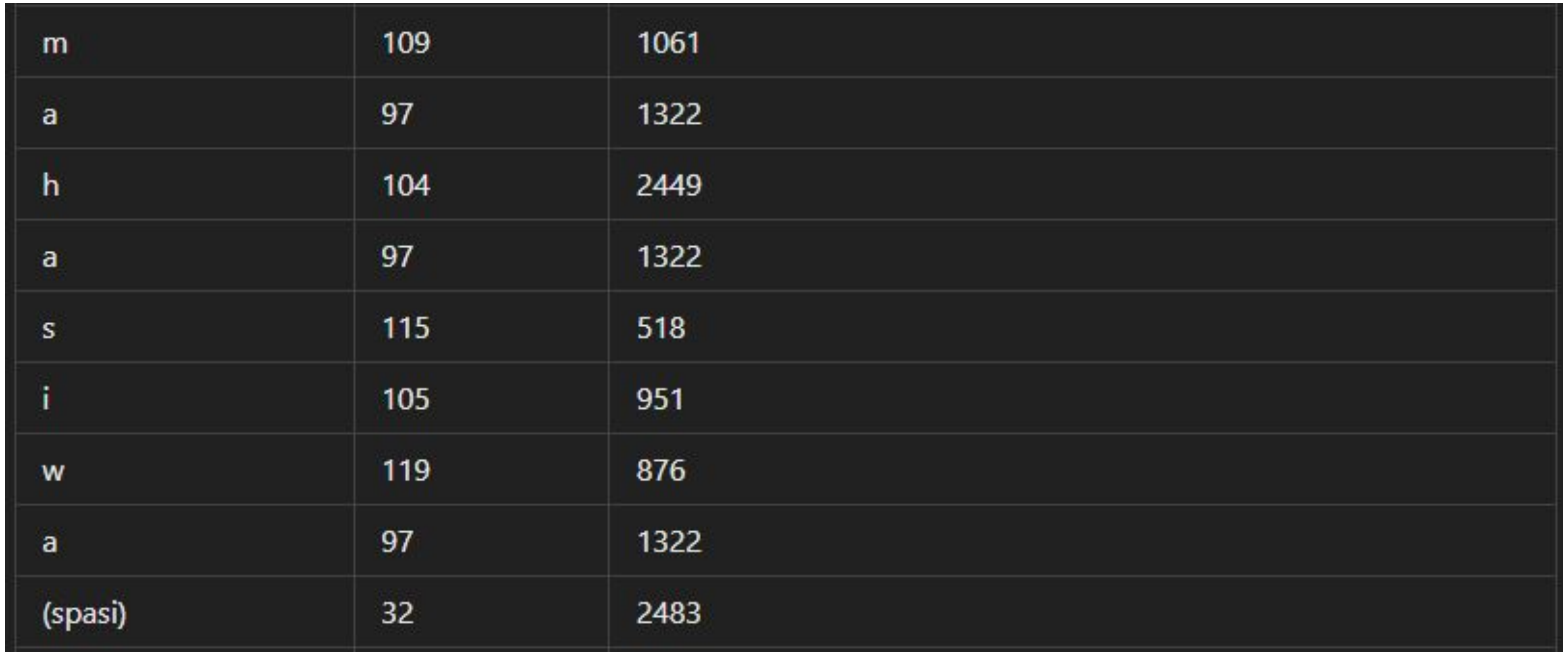
Do the same steps for each message character.



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)

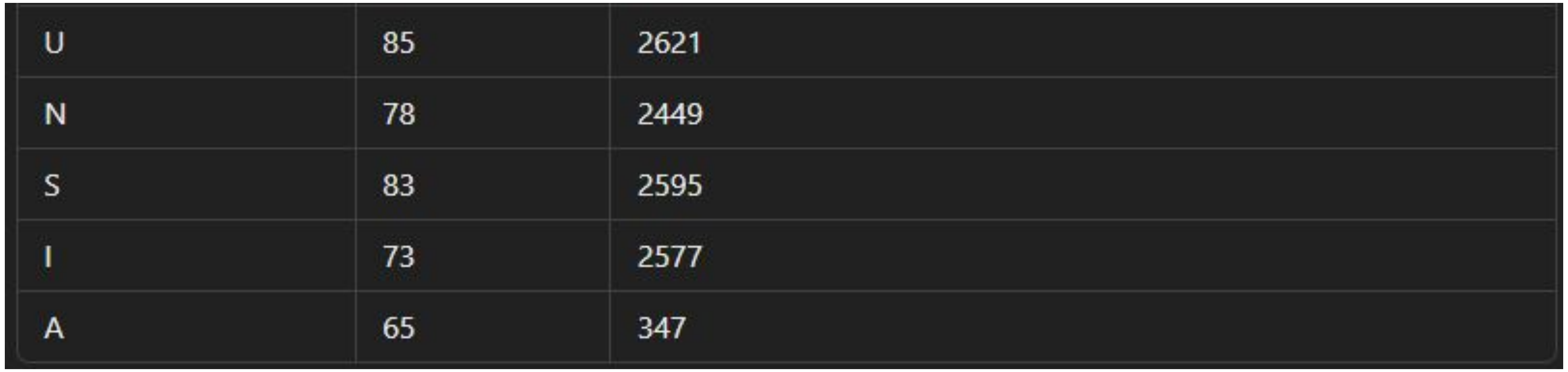
Do the same steps for each message character.



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)

Decryption Using Private Key d=2753 and n=3233

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

Where:

- M is the original message that has been decrypted,
- C is a cipher that has been encrypted,
- d is the private key, dan
- n is modulus.

Rivest-Shamir-Adleman (RSA)

- First Character Decryption: 2595

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

- Perform calculations in stages using the stepped exponent method.
- For example, we can calculate $2595^{2753}\ mod\ 3233$ and get the result, which will return the ASCII value to 'S'.
- The decryption process for other characters can be done similarly.
- After decrypting all the ciphers, we get back the original message:

"Saya adalah mahasiswa UNSIA".

Strength of Asymmetric Cryptography

1. High level security.
2. No need to exchange secret keys.
3. High scalability.

Weaknesses of Asymmetric Cryptography

1. Slow speed.
2. Requires high computing power.
3. Large key size.
4. Reliance on 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)