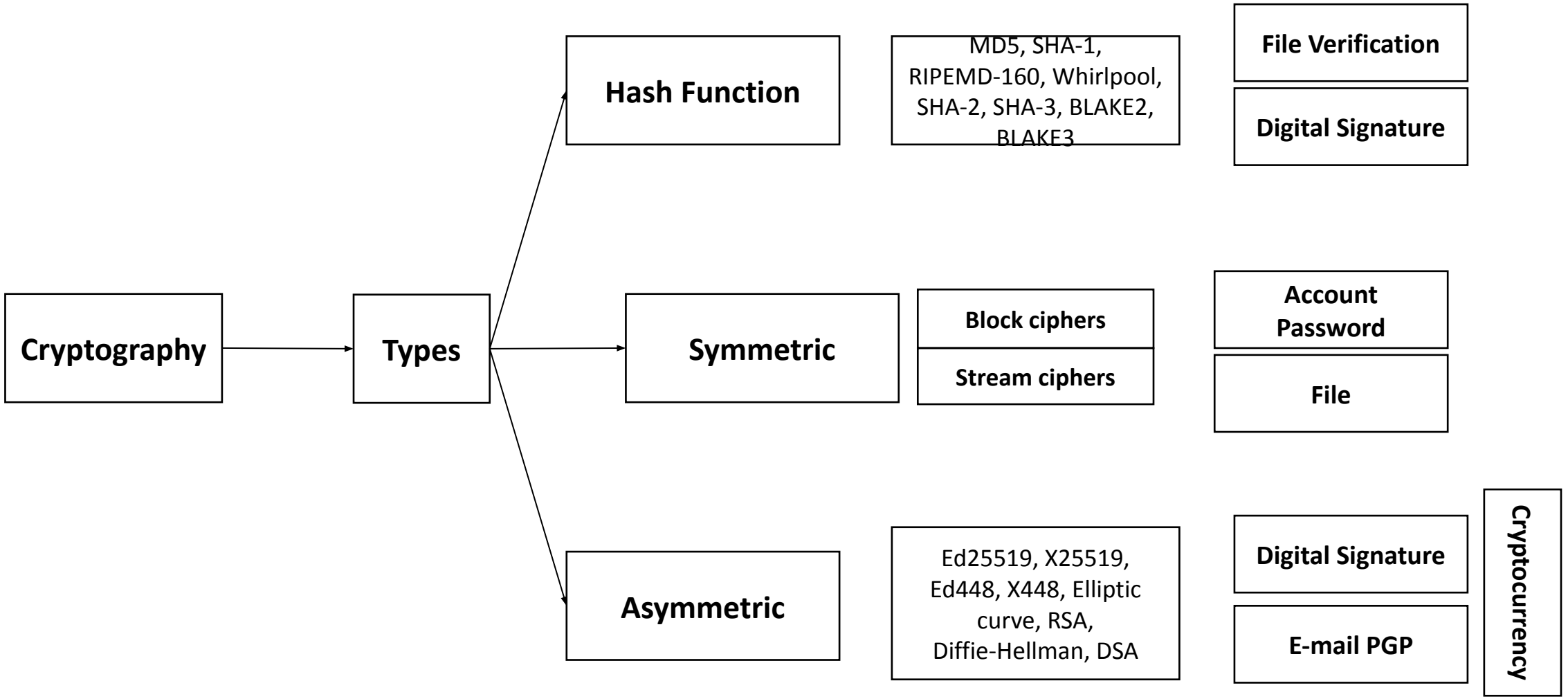
KRIPTOGRAFI DAN STEGANOGRAFI

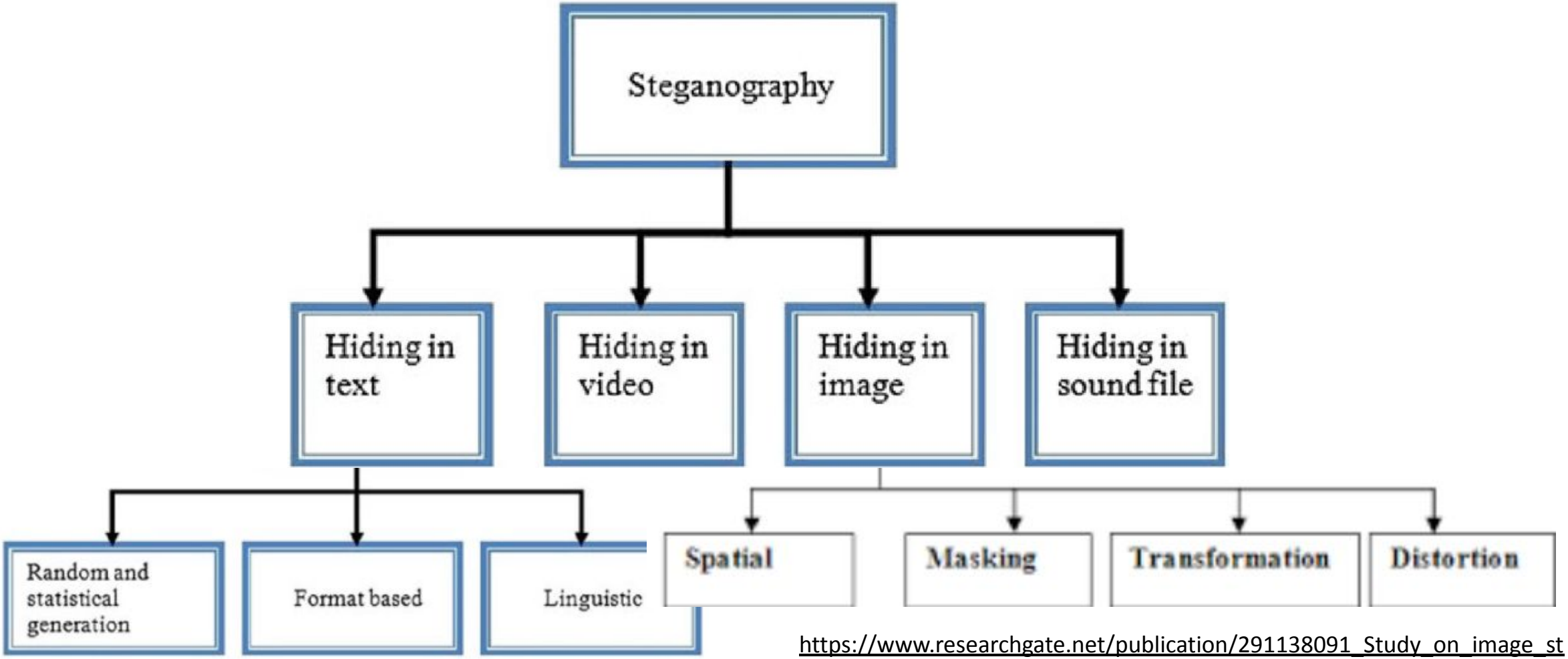
Program Studi Informatika

Sesi 3 – Kriptografi Hash

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

Refreshment Sesi 2


Cryptography
Types
Hash Function
MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2, BLAKE3
File Verification
Digital Signature
Symmetric
Block ciphers
Stream ciphers
Account Password
File
Asymmetric
Ed25519, X25519, Ed448, X448, Elliptic curve, RSA, Diffie-Hellman, DSA
Digital Signature
E-mail PGP
Cryptocurrency

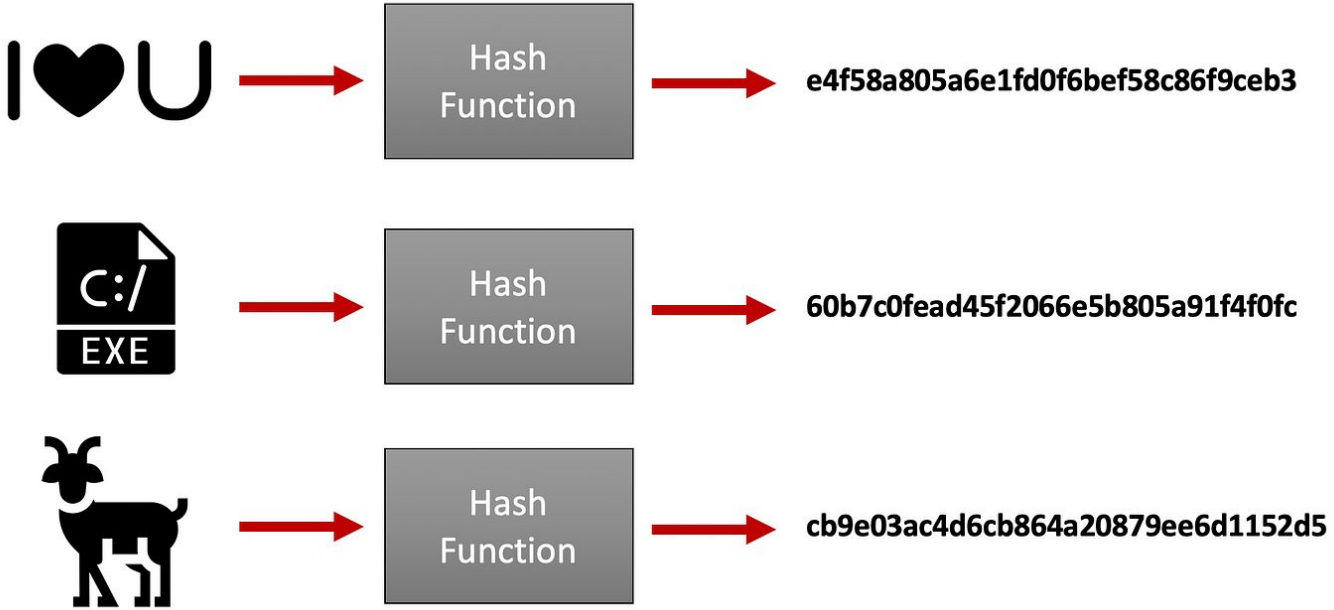


https://www.researchgate.net/publication/311772678_AH4S_An_algorithm_of_text_in_text_steganography_using_the_structure_of_omega_network

https://www.researchgate.net/publication/291138091_Study_on_image_steganography_techniques

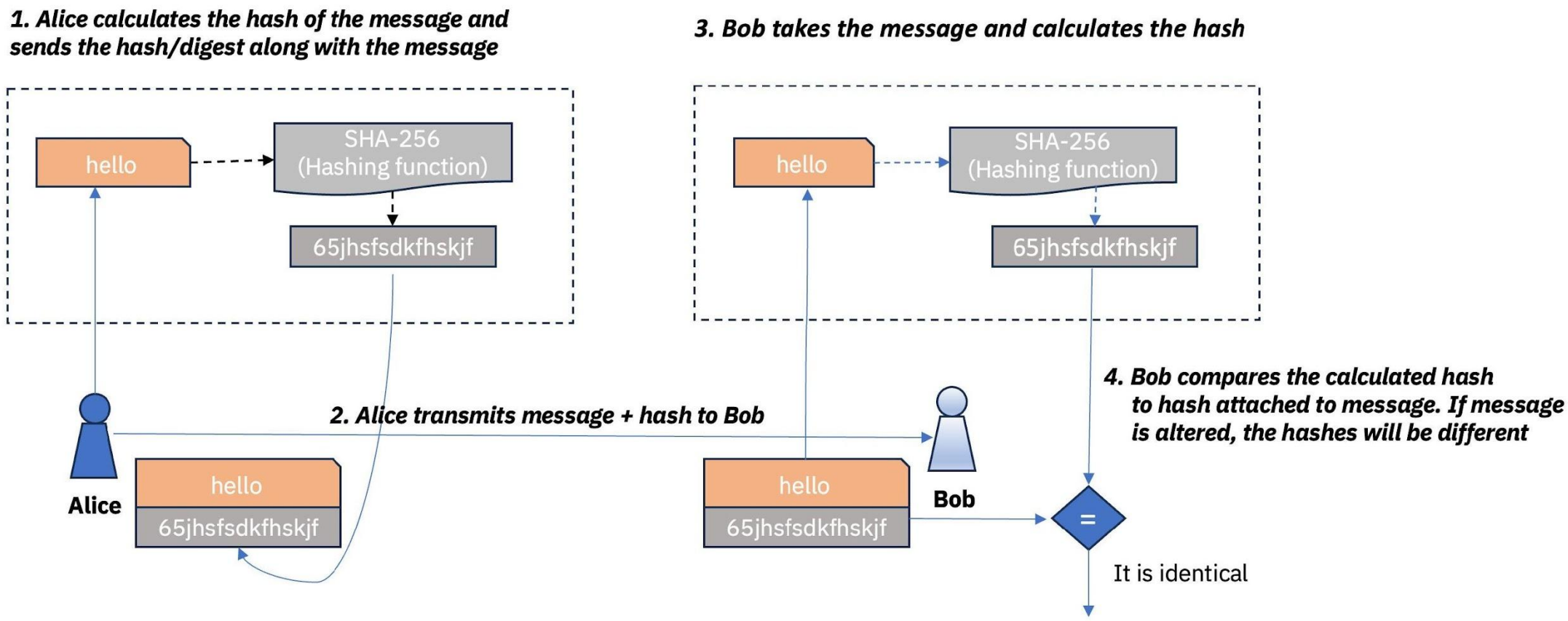
Kriptografi Fungsi Hash

Hash function adalah fungsi matematis yang mengubah data dari ukuran berapa pun menjadi keluaran (output) dengan ukuran tetap yang biasanya berupa string karakter alfanumerik atau angka biner.

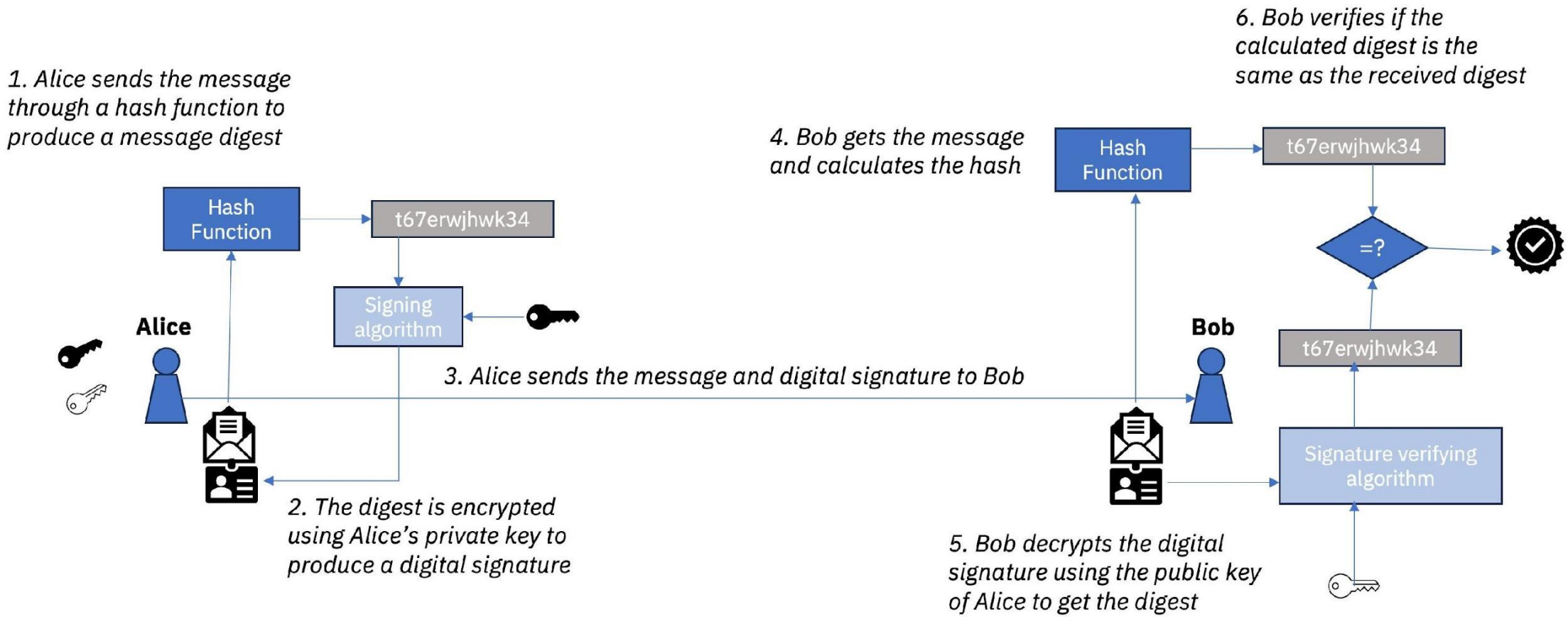


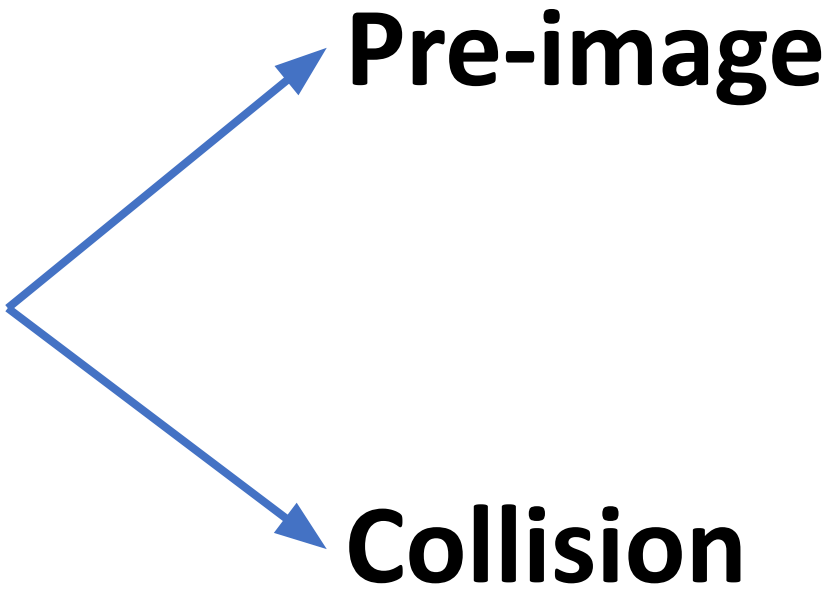
Sumber gambar: SecurityBreak

1. Integritas Data



2. Tanda Tangan Digital




Keamanan
Kriptografi Hash
Pre-image
Collision

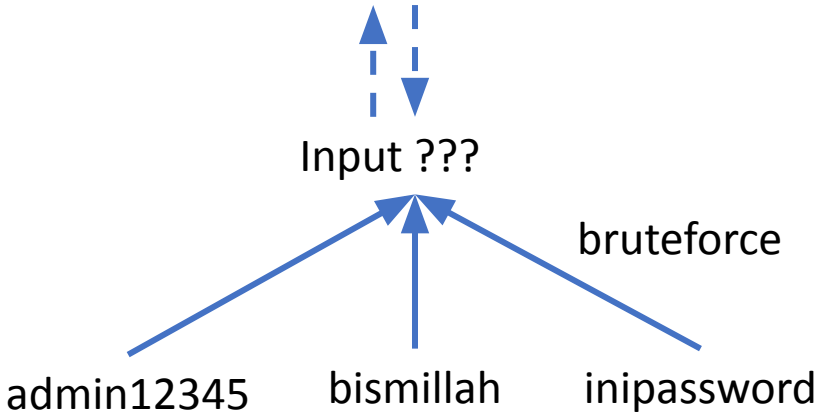
Pre-image resistance (Tahan Pre-image)

Konsep ini mengacu pada kesulitan menemukan input asli jika hanya diberikan nilai hash.

Jika ada sebuah nilai hash $H(x)$ maka sangat sulit untuk menemukan nilai x yang menghasilkan hash tersebut.

Example
Pre-image resistance

Hash:
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd0fa4
d8969d3f80a95



Collision resistance (Tahan Tabrakan)

- Collision resistance berarti sulitnya menemukan dua input berbeda, x dan y dengan $x \neq y$, yang menghasilkan nilai hash yang sama $H(x) = H(y)$.

Example
Collision resistance

HASH $H(x) = H(y)$:
59266e8b0ae7f28babf85df
d54653f33695d04bcfc944
48985c5e3fa15a85ba6

HASH x:
51ac881397b1afb277a1ba
19e97f688efd6cab5ae4f2f
175c6f9e0e34fd74d31

HASH y:
06a1ed7fee6aa51f7d2f9b6
6c070fd8a23ef064702c04
d9ed56a18f3468e259c

Demo

https://colab.research.google.com/drive/1xSGLG7gMOfzet-zqxPMmrJgoefdCav5r?usp=sharing

Kelemahan Kriptografi Hash

1. Pre-image Attack
2. Collision Vulnerability
3. Length Extension Attack
4. Rainbow Table Attack
5. Brute-force Attack
6. Tidak Reversible

Mengurangi Kelemahan Kriptografi Hash

1. Hindari menggunakan algoritma hash yang sudah tidak aman (seperti MD5 dan SHA-1) untuk keperluan keamanan. Pilih algoritma yang lebih aman seperti SHA-256, SHA-3, atau algoritma khusus password seperti bcrypt, scrypt, atau argon2.
2. Penggunaan salt (data acak) pada input sebelum hashing membantu melindungi dari rainbow table attack dan membuat setiap hash unik.
3. Memilih algoritma hash dengan panjang output yang lebih besar mengurangi kemungkinan collision dan membuat brute-force attack lebih sulit dilakukan.
4. Gunakan metode hashing yang melibatkan banyak iterasi (pengulangan) seperti pada bcrypt atau argon2 dapat memperlambat proses hashing dan membuat brute-force attack lebih sulit dan memakan waktu lama.

- 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)