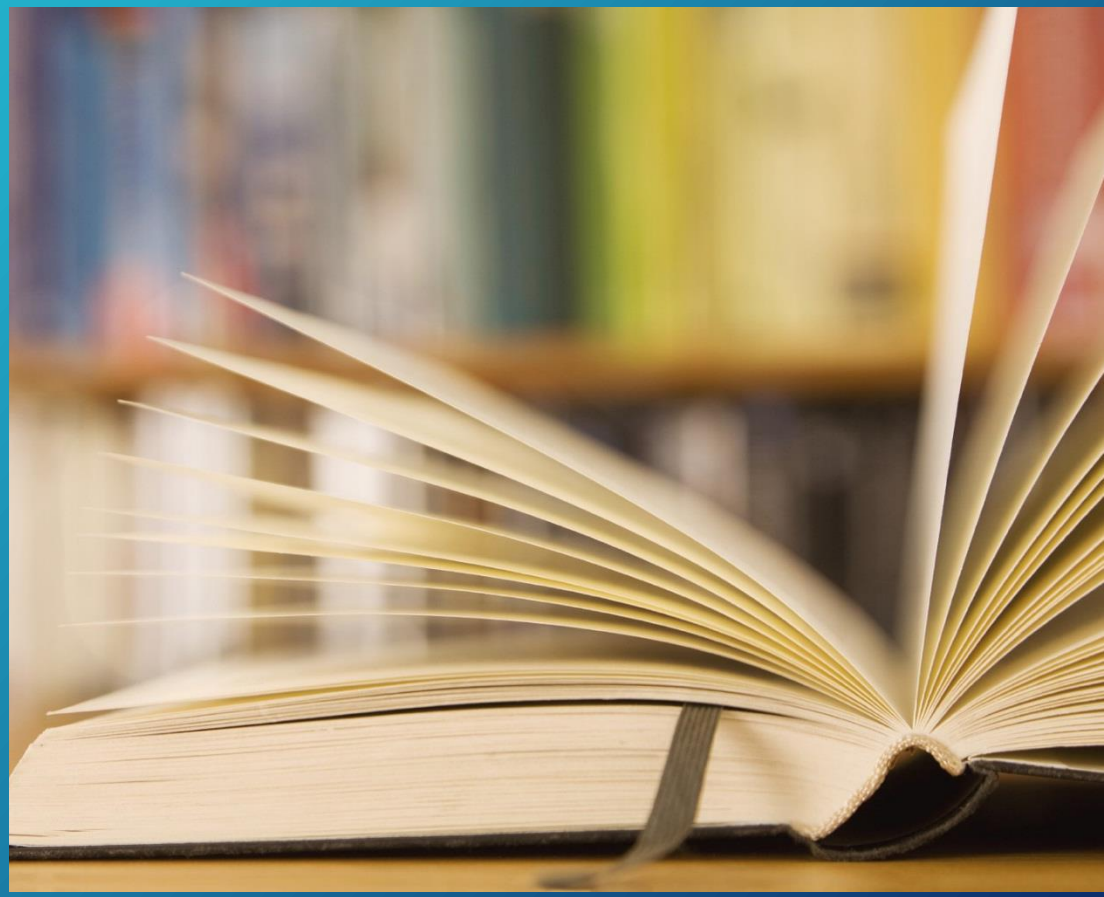
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

DASAR KEAMANAN KOMPUTER

Keamanan Sistem Informasi – Aditya Putra, ST., MT.



Agenda

- Access Control
  - Authentication
  - Authorization
- Cryptography
  - Enkripsi
  - Hash
- Protokol
  - IPSec
  - TLS
  - SSH
- Keamanan Jaringan 1: Proxy
- Keamanan Jaringan 2: Firewall

Authentication

Authentication/otentikasi adalah metode untuk mengidentifikasi apakah seseorang yang akan masuk ke dalam sistem user yang benar atau tidak

Metode Otentikasi setidaknya ada 3 kategori:

- **Something you know**: Password, PIN, kombinasi kunci, nama ibu, warna favorit, dll
- **Something you have:** Smart Card, Device Token, Lokasi/Koordinat, dll
- **Something you are:** Fingerprint, Voice print, Retina, Iris, Bentuk Wajah, Telapak Tangan, Pola Berjalan, dll

Pada implementasi *two-factor authentication (TFA)*, otentikasi yang digunakan wajib menggunakan 2 metode yang berbeda kategori

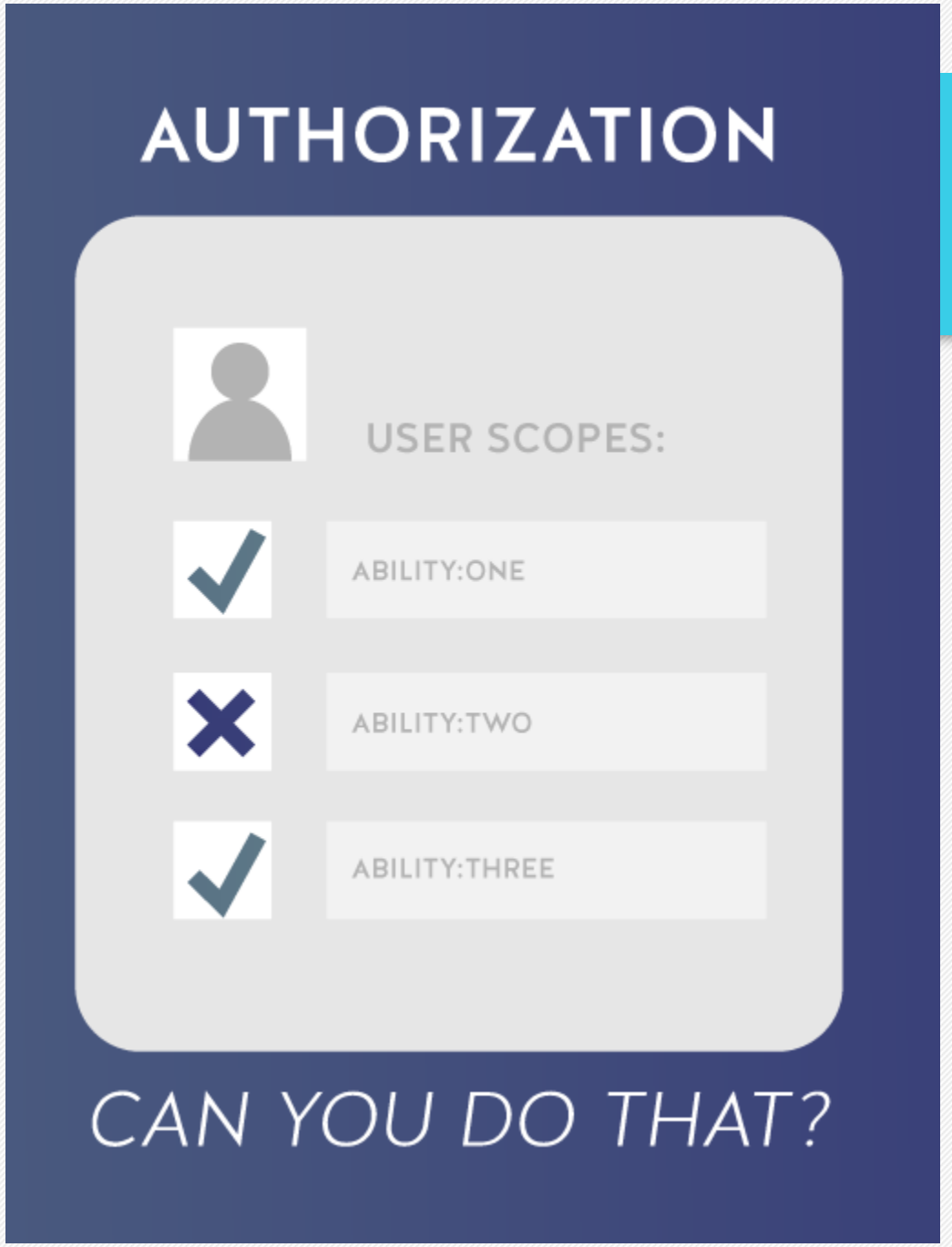
Authorization

Authorization/otorisasi adalah pemberian hak kepada user setelah login/masuk ke dalam sistem. Sehingga user hanya melakukan aktivitas, mengakses data, dan layanannya sesuai dengan privilege-nya

Dengan demikian, seseorang yang telah terotentikasi ke dalam sistem belum tentu memiliki akses ke setiap aktivitas/data/layanan yang ada

Pada otentikasi seorang user diberikan akses secara 1/0 atau *totally* diberikan atau tidak. Sedangkan otorisasi memberikan akses secara custom tergantung priviledge-nya

Otentikasi → Siapa anda?
Otorisasi → Apa anda bisa melakukannya?



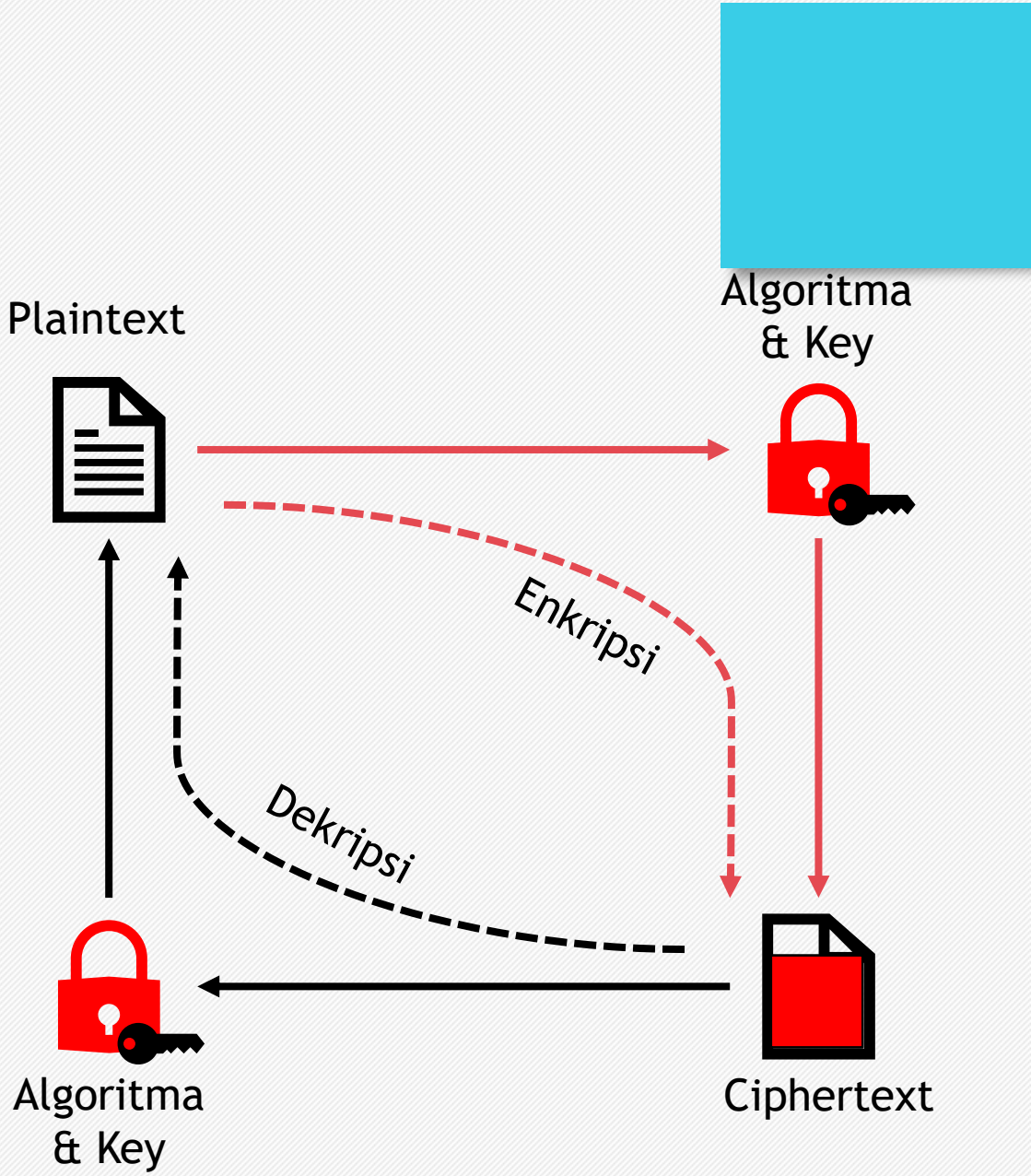
Enkripsi

Enkripsi adalah proses untuk mengubah pesan atau teks asli *(plaintext)* menjadi *ciphertext* sehingga informasi yang terkandung pada teks tersebut tersembunyi.

Elemen dari Enkripsi

- **Algoritma** adalah fungsi yang digunakan untuk melakukan enkripsi dan dekripsi
- **Key** adalah salah satu factor yang menentukan kekuatan suatu enkripsi
- **Plaintext** merupakan pesan atau teks asli
- **Ciphertext** teks output hasil enkripsi

Enkripsi bersifat dua arah. Artinya Ciphertext dapat dikembalikan menjadi Plaintext dan proses ini dikenal dengan **Dekripsi**

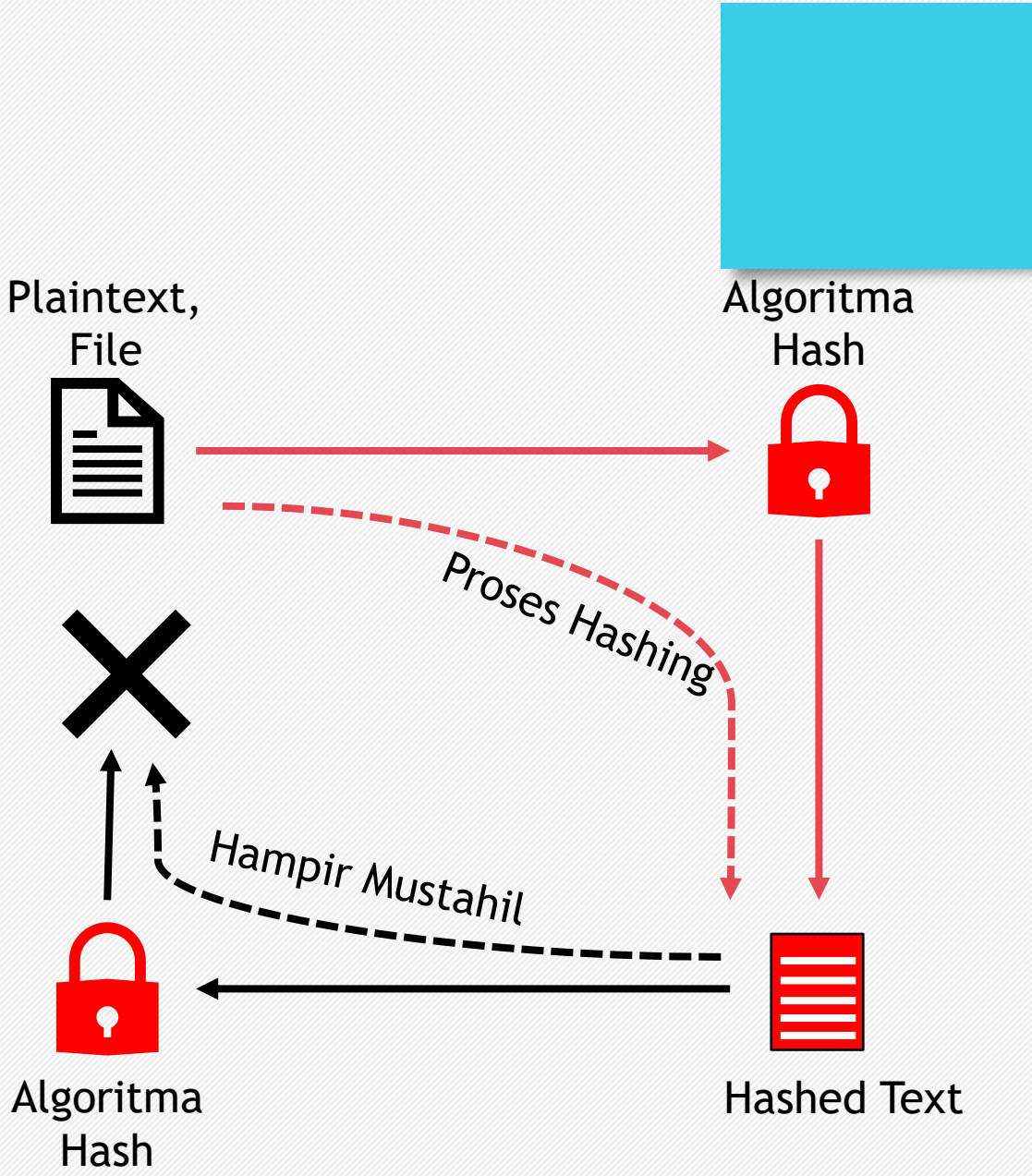


Hash (1)

Berbeda dengan enkripsi, Hash adalah fungsi yang bersifat 1 arah atau dengan kata lain, *hashed text* hampir mustahil untuk bisa dikembalikan kembali menjadi *plaintext*

Perbedaan lain antara Hash dan enkripsi adalah tujuannya. Tujuan yang ingin dicapai enkripsi adalah *CONFIDENTIALITY*, maka pada Hash yang ingin dicapai adalah *INTEGRITY*

Dari awal, Enkripsi dilakukan untuk mengamankan informasi supaya jika data berhasil disadap atau dicuri maka nilai informasinya masih terjaga. Sehingga hanya pemilik sah dari data itu saja yang mampu untuk mendekripsikannya Kembali. Ini tujuan CONFIDENTIALITY-nya



Hash (2)

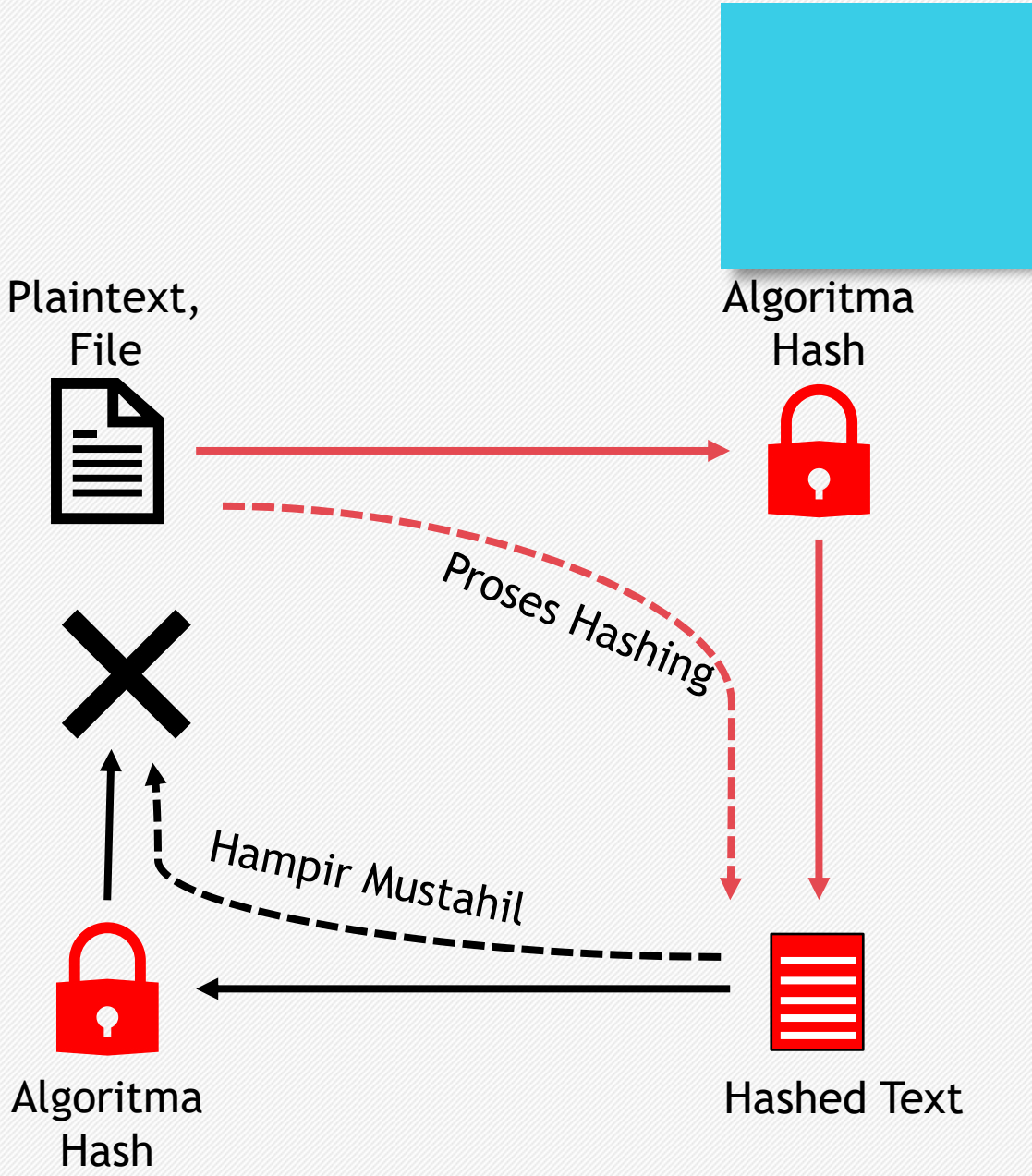
Hash menjaga informasi bukan dengan menjaga kerahasiaannya, namun dengan menjamin bahwa data tetap terjaga keasliannya

Cara Kerja

- Proses Hash dilakukan pada sebuah teks (*plaintext*)
- Proses tersebut menghasilkan Hashed Text yang unik

Hash menghasilkan nilai yang sangat unik terhadap sebuah data/teks/file yang diberikan. Karena perubahan 1 karakter saja pada data akan menghasilkan nilai Hash yang berbeda.

Di sini letak tujuan INTEGRITY-nya. Hash memastikan bahwa suatu data/file *legitimate* atau tidak



Protokol IPSec

- IPSec adalah kumpulan protocol yang dijadikan standar oleh Internet Engineering Task Force (IETF) dan berada dalam layer network
- IPSec berasal dari IP (singkatan dari Internet Protocol) dan Sec (Security). IPSec dianggap secure/aman karena menambahkan enkripsi dan otentikasi pada prosesnya. Untuk itu, sering digunakan pada teknologi VPN (Virtual Private Network)
- Protokol yang digunakan IPSec adalah
  - **Authentication Header (AH),** menentukan paket header opsional yang digunakan untuk menjamin integritas dan otentikasi asal data pada paket IP dan untuk mencegah *replay attack*
  - **Encapsulating Security Payload (ESP),** memberikan header paket yang digunakan untuk menyediakan enkripsi paket, proteksi integitas data, otentikasi asal data, access control,
  - **Internet Key exchange (IKE),** protocol yang memungkinkan host tuntuk menentukan layanan mana yang diakan digunakan pada paket. Layanan yang dimaksud adalah algoritma kriptografi dan mekanisme sharing key dengan algoritma tersebut

Cara Kerja IPSec

1. Host mengenali paket mana yang perlu ditransmisikan menggunakan IPSec. Lalu host akan melakukan rangkaian security policy terhadap paket yang berarti memastikan bahka paket akan dikirimkan menggunakan enkripsi dan/atau otentikasi yang tepat

2. IKE tahap 1. Pada tahap ini, IKE tahap 1 memastikan bahwa antara 2 host (pengirim dan penerima) melakukan negosiasi untuk menentukan, menginisiasi secure circuit, dan saling mengotentikasi. Ada dua opsi pada IKE tahap 1:
    1. Main Mode → lebih secure karena terlebih dulu membangun secure tunnel untuk bertukar algoritma sesi dan key
    2. Aggressive Mode → lebih cepat karena algoritma sesi dikirimkan dalam bentuk plaintext

3. IKE tahap 2 memastikan algoritma kriptografi yang digunakan, secret key, dan Nonce. Ketika kedua host sudah sepakat, IKE Security Association (SA) akan dibangun yang mendefinisikan IPSec Tunnel. Host juga dapat memastikan forward secrecy pada tahap ini

4. Pertukaran data menggunakan channel terenkripsi yang sudah dibangun. Enkripsi dan dekripsi dilakukan oleh kedua host berdasarkan SA yang dilakukan pada langkah2 sebelumnya

5. Terakhir, Ketika komunikasi sudah selesai, IPSec tunnel akan dihancurkan

Protokol TLS

- Transport Layer Security (TLS) adalah protocol kriptografi yang untuk memfasilityas keamanan privasi dan data untuk berkomunikasi di internet
- Penggunaan paling umum adalah enkripsi pada komunikasi antar web aplikasi dengan server. Namun TLS juga digunakan pada email, messaging, dan VoIP
- TLS adalah suksesor dari Secure Socket Layer (SSL) yang telah dihentikan pengembangan dan penggunaannya.
- TLS 1.0 sebenarnya adalah SSL 3.1, namun penggantian namanya menjadi TLS digunakan sebagai indikasi tidak adanya asosiasi lagi dengan Netscape sebagai developer pertama SSL.
- TLS menjalankan 3 fungsi pengamanan:
  - Encryption: menyembunyikan data dari pihak ketiga
  - Authentication: memastikan informasi hanya bisa diakses oleh pihak yang tepat
  - Integrity: verifikasi bahwa data tidak diubah ditengah jalan
-

Cara Kerja TLS

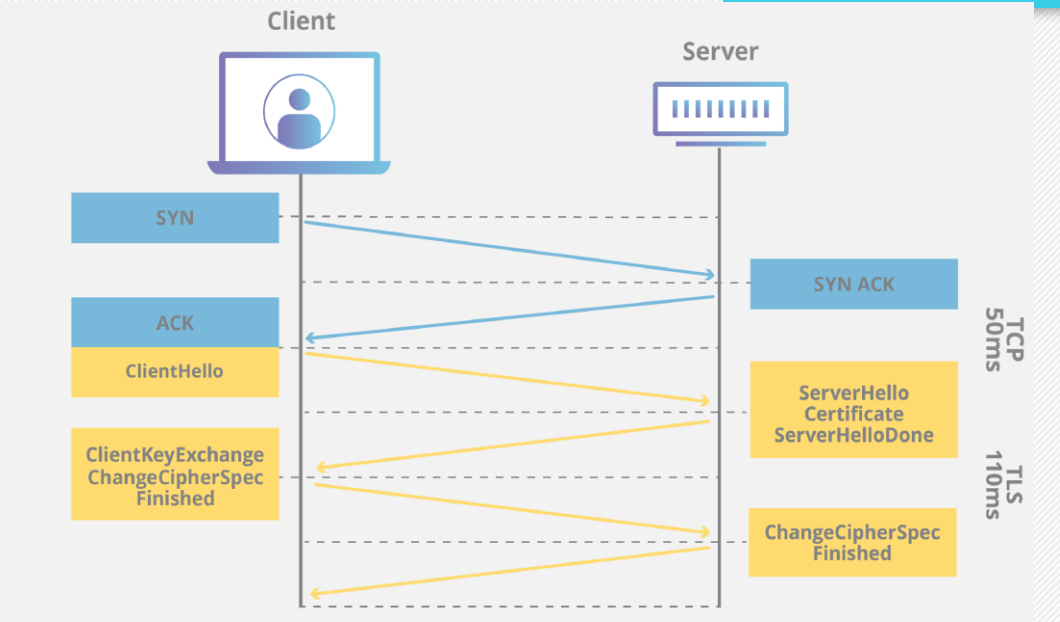
- Website atau aplikasi yang menggunakan TLS harus memiliki sertifikat TLS pada servernya yang menyatakan kepemilikan domain

- Sebuah koneksi TLS dibangun menggunakan TLS handshake. Berikut yang dilakukan pada tahap TLS handshake
  - Menentukan versi TLS yang digunakan
  - Menentukan cipher suite yang digunakan
  - Otentikasi idetitas server menggunakan server TLS
  - Mengeluarkan session key untuk enkripsi pesan antara client dan server

- TLS handshake membangun cipher suite untuk tiap sesi komunikasinya.

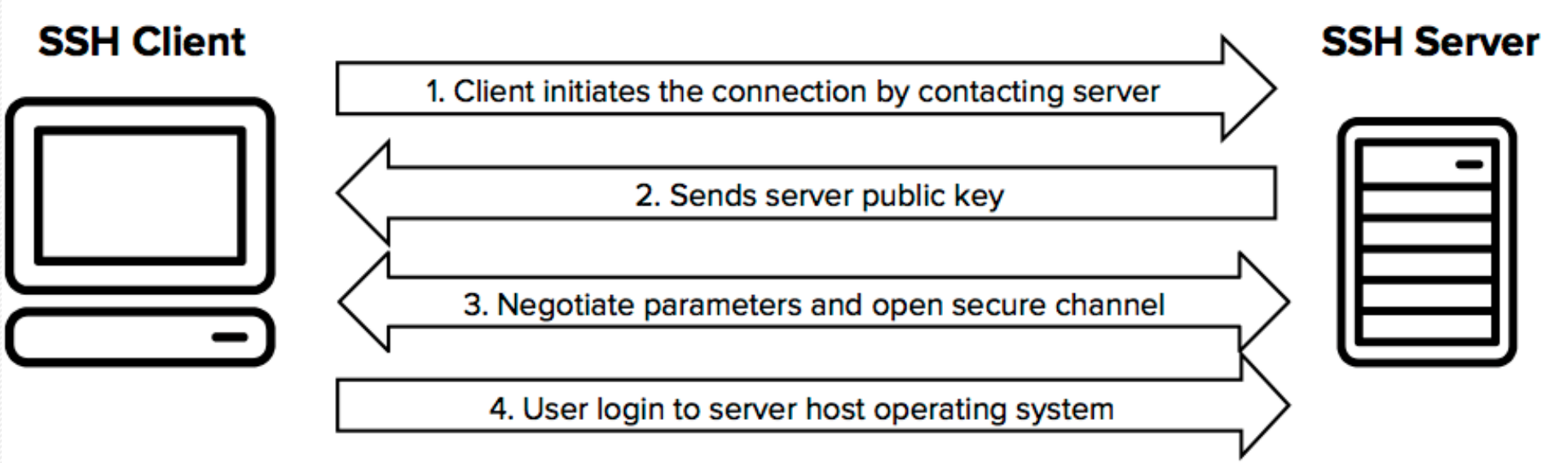
- TLS handshake juga mengatur otentikasi yang menjamin identitas server kepada client-nya

- Ketika data telah dienkripsi dan diotentikasi, data lalu di-”tandatangani” menggunakan Message Authentication Code (MAC) yang berfungsi untuk menjadi orisinalitas atau integritas data.



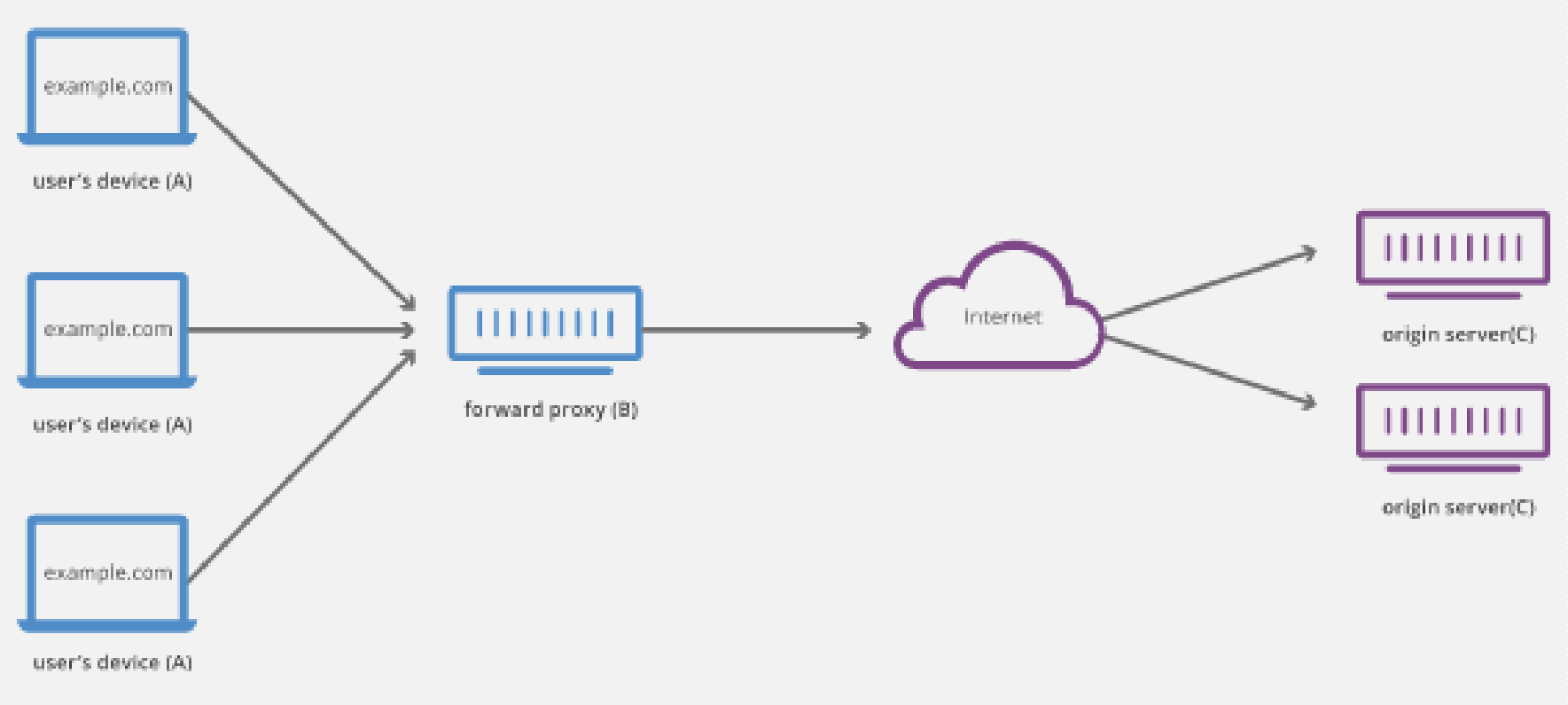
Protokol SSH

- Secure Shell (SSH) adalah protokol secure remote login dari klien ke server menggunakan default port 22. SSH menjadi solusi alternatif yang aman dibandingkan dengan protocol login lain seperti telnet dan rlogin
- SSH diimplementasikan dalam layanan lain sepertif Secure File Transfer Protocol (SFTP)
- Protokol SSH bekerja dengan model client-server. Koneksi diinisiasi oleh klien untuk tersambung ke server menggunakan public key cryptography untuk memverifikasi identitas server SSH.



Keamanan Jaringan: Proxy

- Proxy atau Web Proxy adalah server yang berada di depan sisi grup mesin client. Ketika client tersebut hendak mengakses suatu situs dan service di internet, proxy yang berada di depannya meng-intercept request tersebut dan memforwardnya kepada situs yang dimaksud sebagai perwakilan klien tadi.



Keamanan Jaringan: Proxy

Lalu mengapa perlu ada middleware seperti ini? Ada beberapa alasan dan benefit penggunaan proxy

- Menghindari pembatasan akses yang dilakukan oleh institusi/pemerintah
  Ketika ada suatu situs yang dilarang oleh pemerintah karena suatu alasan politik misalkan, pengguna dapat mem-bypassnya dengan proxy. Tentu ini harus dengan kondisi proxy terletak di luar wilayah kewenangan institusi/pemerintah

- Block access suatu konten tertentu
  Sebagai pihak pemilik proxy, penggunaannya juga bisa dipakai untuk keperluan sebaliknya. Yaitu membatasi akses terhadap konten atau situs tertentu

- Untuk melindungi identitas online personal
  Penggunaan proxy membuat identitas user seolah berasal dari IP proxy bukan IP sebenarnya. Sehingga menghindarkan dari tracing back ke IP asli

Keamanan Jaringan: Firewall

- Firewall adalah perangkat filtering network yang digunakan untuk monitoring trafik yang dating dan pergi dan menentukan apakah suatu trafik diizinkan lewat atau tidak berdasarkan serangkaian security rules. Seiring perkembangannya, Firewall berkembang menjadi tak hanya berupa hardware, namun juga software.

- Ragam Firewall
  - Statefull Firewall → tradisional firewall yang bekerja berdasarkan parameter state, port, protocol
  - Unified Threat Management → kombinasi antara firewall dengan Intrusion Prevention dan Antivirus
  - Next-generation Firewall → firewall yang telah berkembang lebih dari tradisional FW. Berdasarkan definisi Gartnet, Inc. NGFW harus memiliki fitur
    - Standar fitur Statefule FW
    - Terintegrasi dengan IPS
    - Application Awareness dan kendali untuk melihat dan block aplikasi yang mencurigakan
    - Fungsi update feed informasi terbaru
    - Teknik yang mampu mencegah bentuk evolusi dari ancaman security