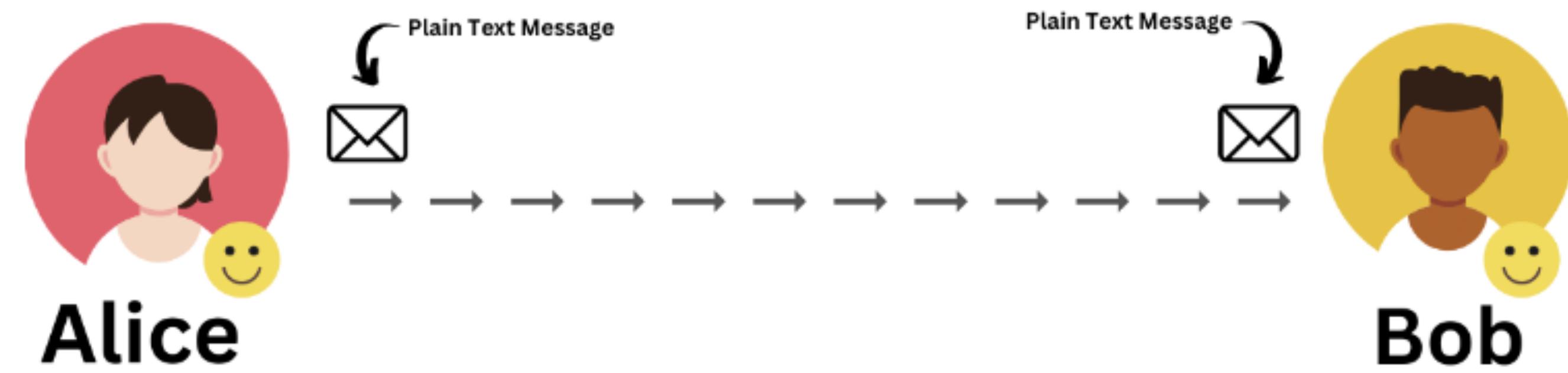


# **Pengantar Kriptografi**

## **Bahan Kuliah Keamanan Data**

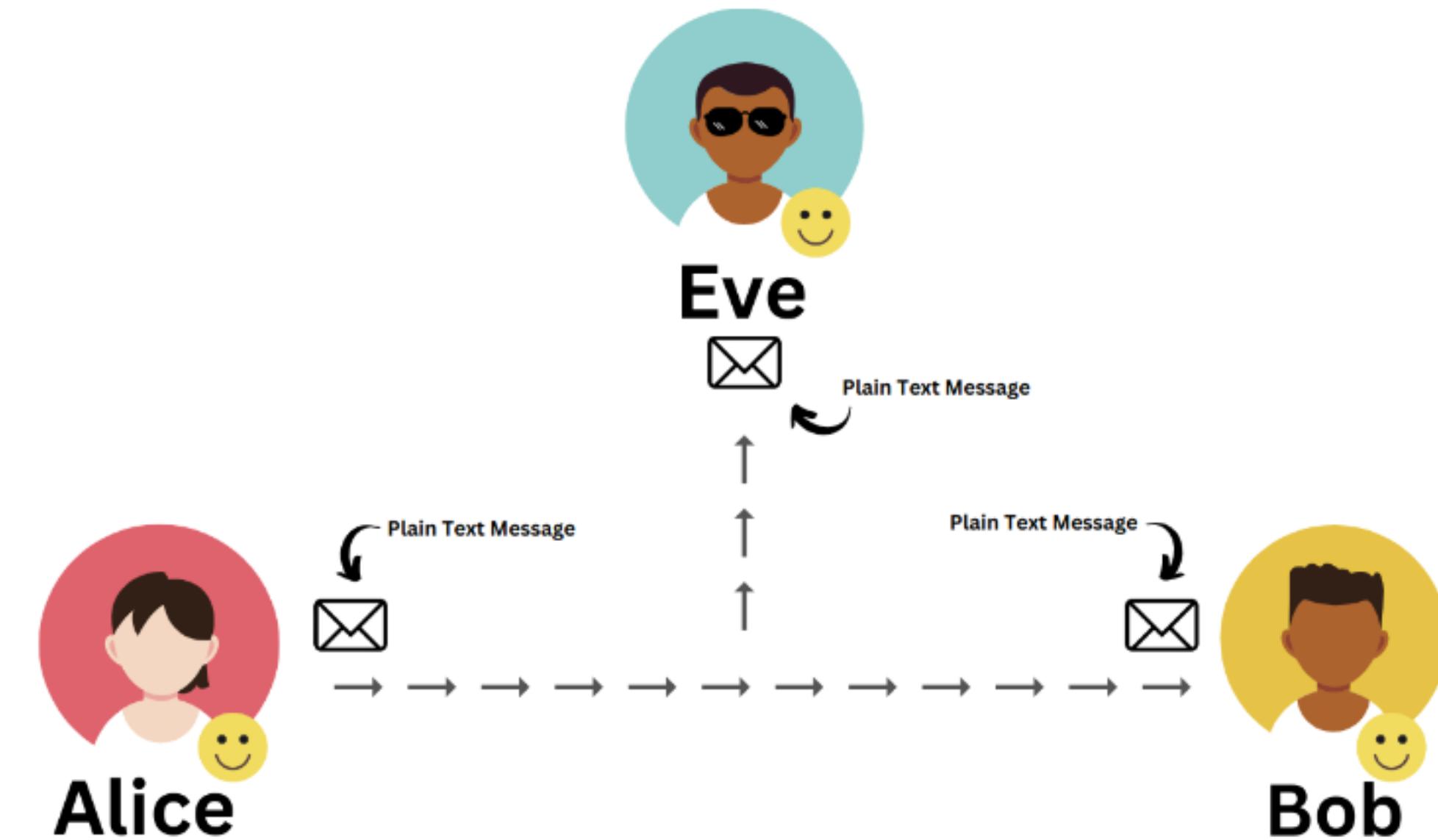
**Sevi Nurafni**

**Fakultas Sains dan Teknologi**  
**Universitas Koperasi Indonesia 2025**



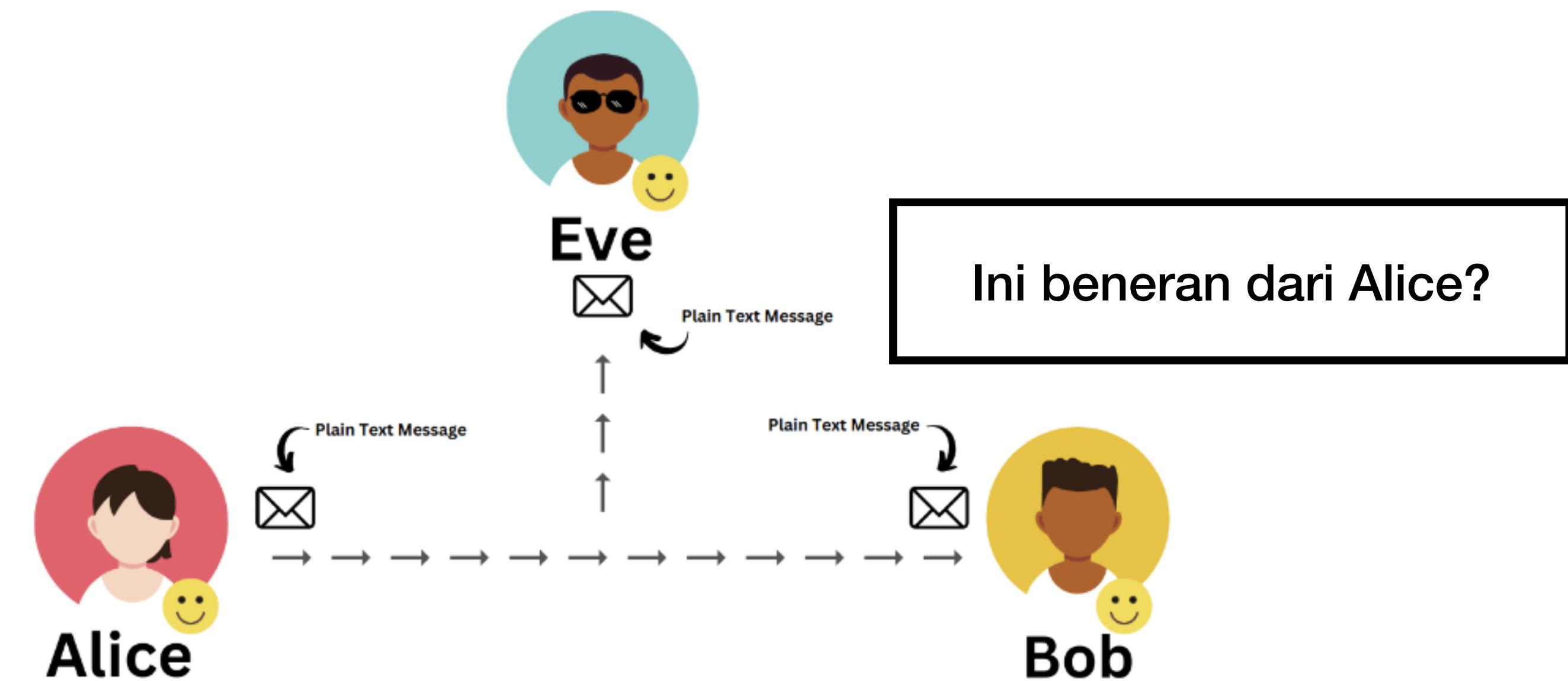
*Diagram 01: Alice sends a plain text message to Bob*

**Case 1:** Bagaimana Alice memastikan setiap pesannya tidak dapat dibaca oleh penyadap (eavesdrooper) yang menguping komunikasi dengan Bob?



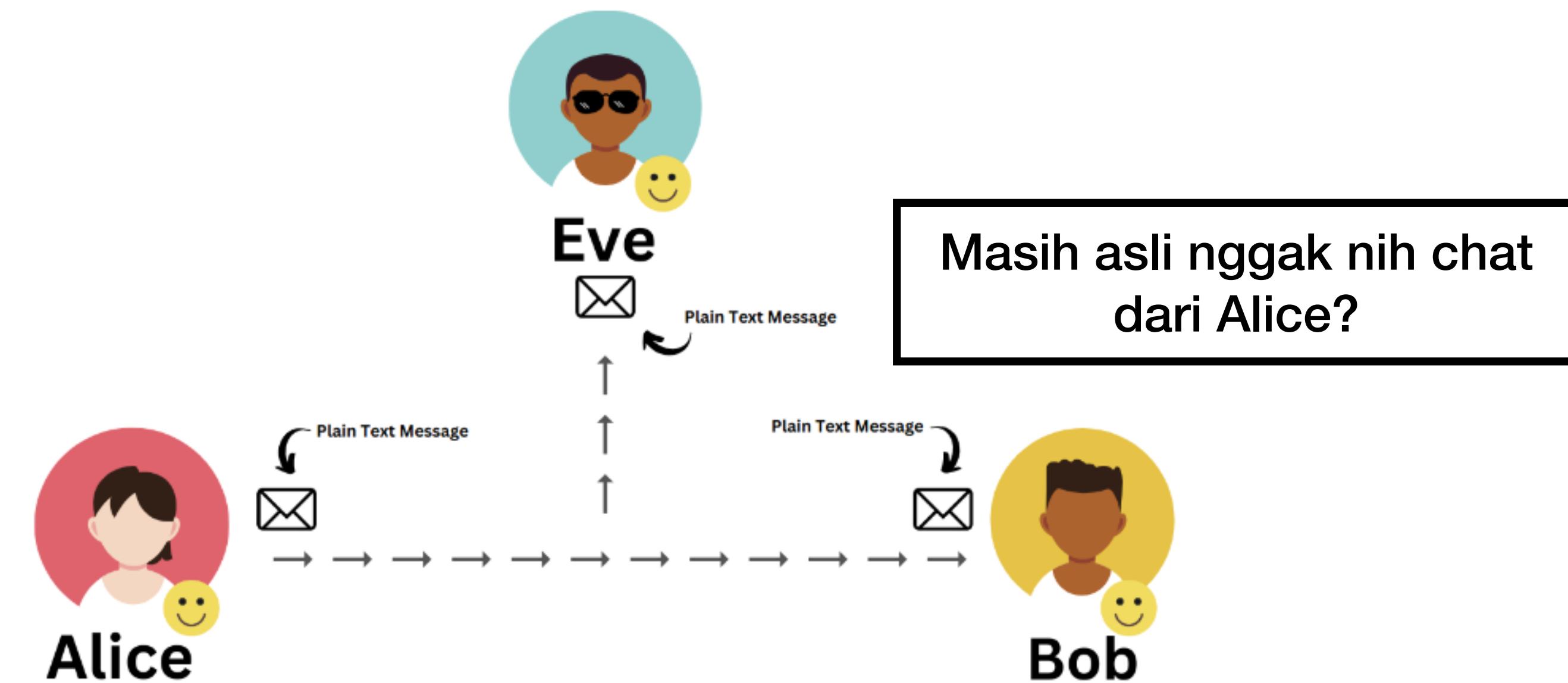
*Diagram 02: Alice sends a plain text message to Bob, Eve reads it*

**Case 2:** Bagaimana Bob memastikan bahwa pesan tersebut dari Alice dan bukan dari Eve (yang menyamar menjadi Alice)?



*Diagram 02: Alice sends a plain text message to Bob, Eve reads it*

**Case 3:** Bagaimana Bob memastikan bahwa pesan dari Alice masih utuh, asli, tidak diubah, atau dimanipulasi selama komunikasi?



*Diagram 02: Alice sends a plain text message to Bob, Eve reads it*

## Case 4: Bagaimana Bob melakukan anti-sangkalan apabila Alice menyangkal sudah mengirim pesan kepada Bob

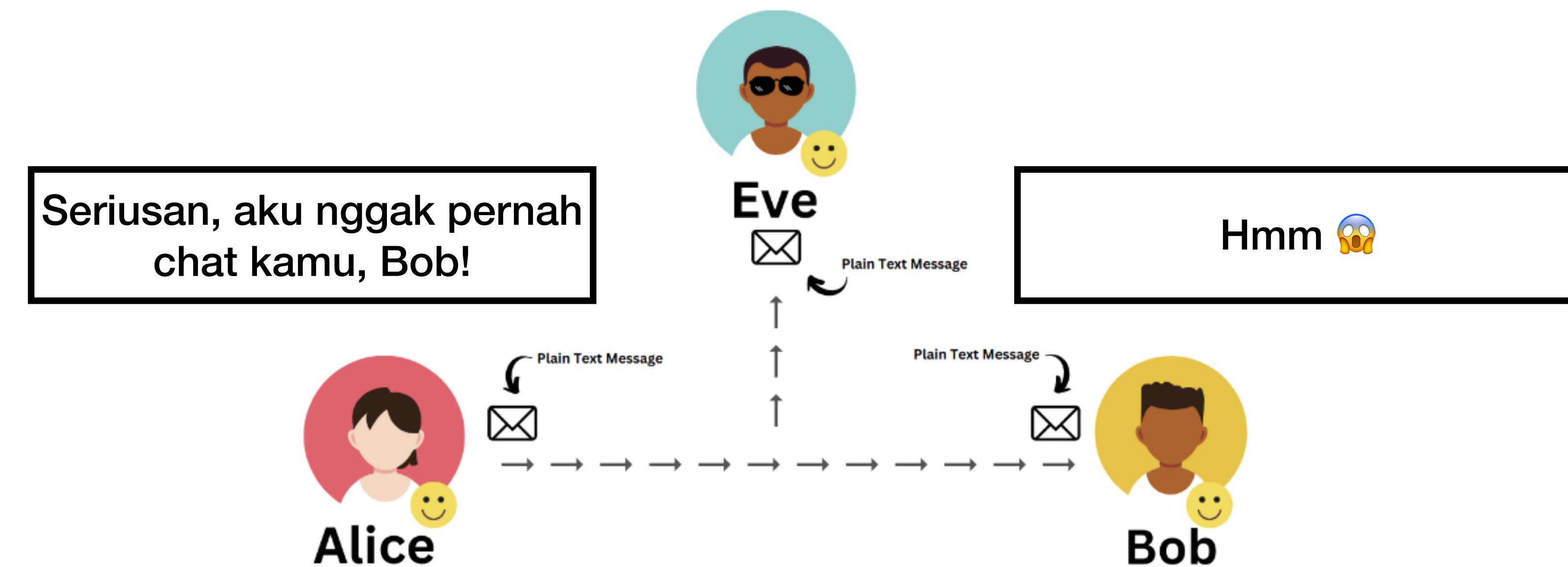


Diagram 02: Alice sends a plain text message to Bob, Eve reads it

Keempat masalah tadi:

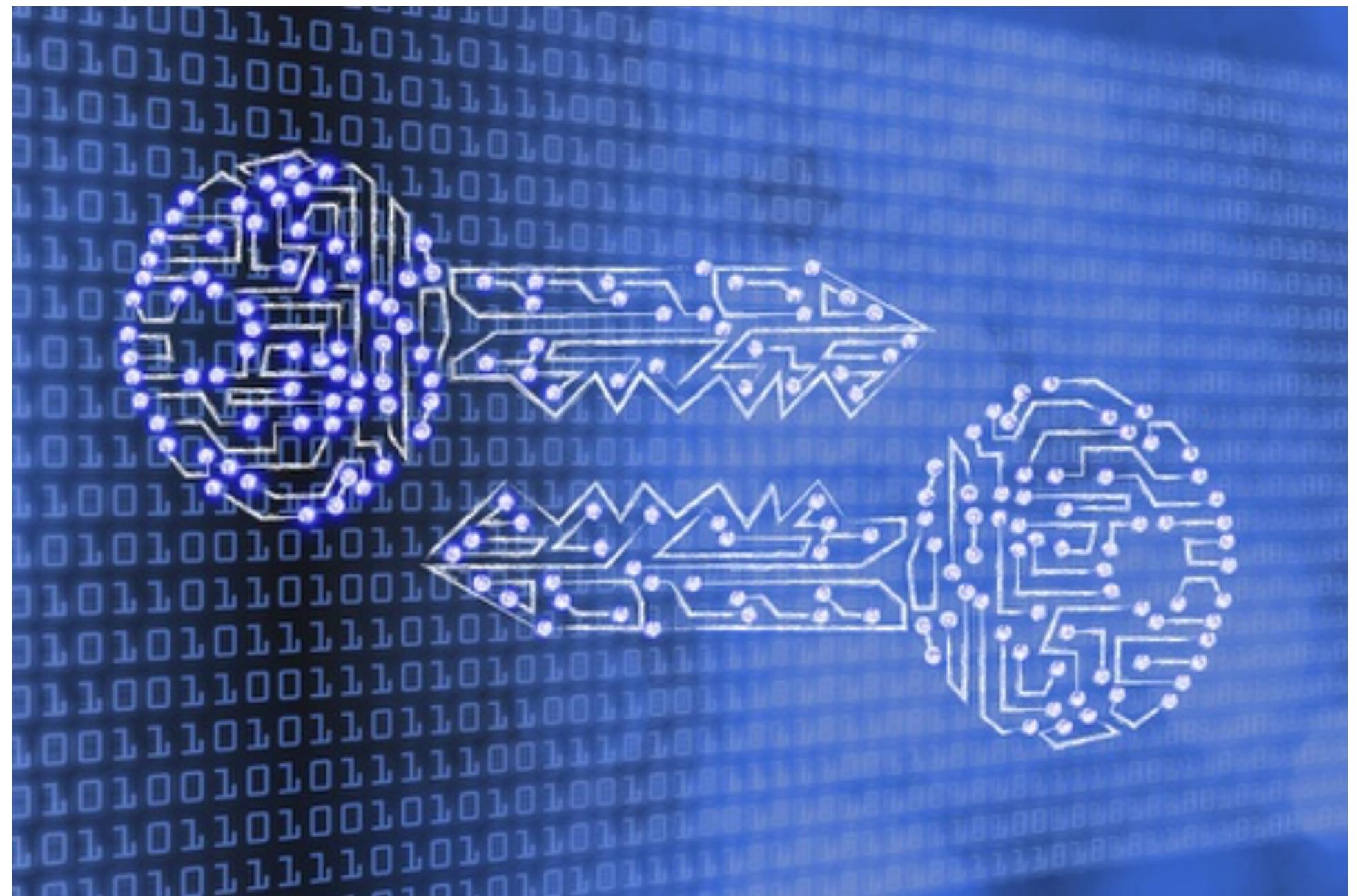
- masalah kerahasiaan pesan
- masalah otentifikasi pengirim atau penerima
- masalah keutuhan (integrity) pesan?

**Solusinya adalah KRIPTOGRAFI**

# KRIPTOGRAFI

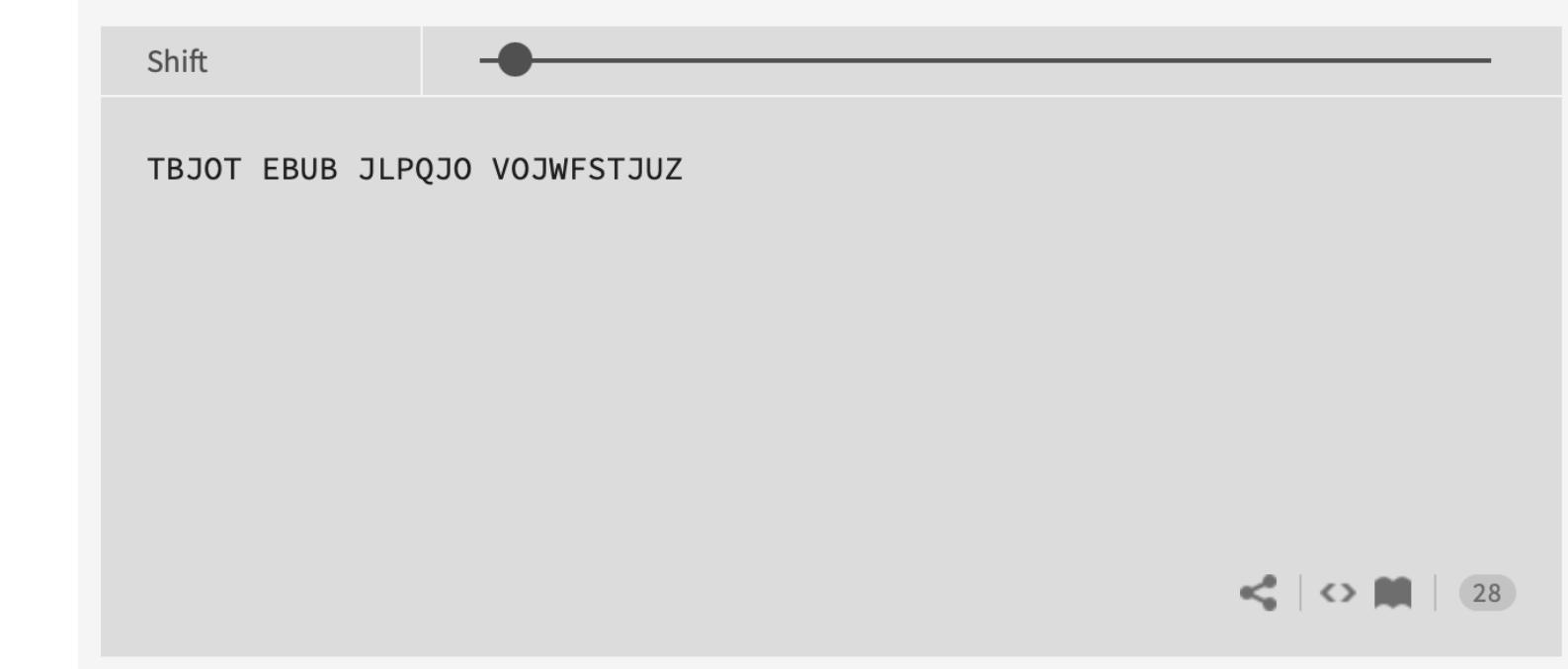
**Kriptografi:** ilmu dan seni untuk menjaga keamanan pesan. (Schneier, 1996)

**Kriptografi:** ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Menez, 1996)

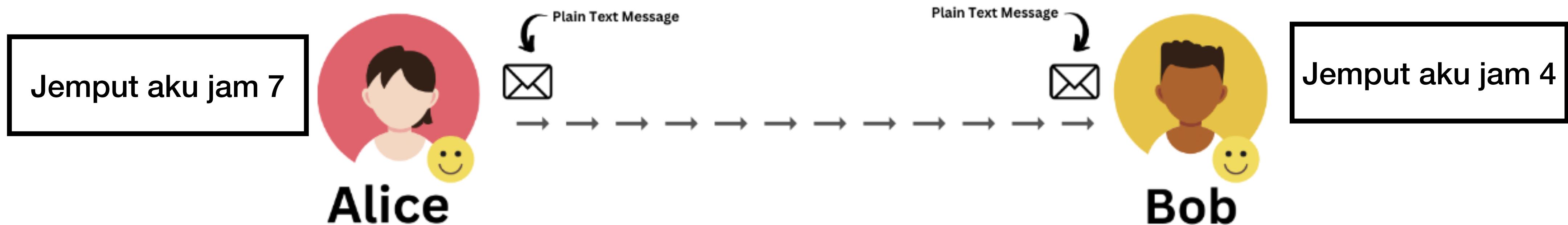


# Aman?

## 1. Terjaganya kerahasiaan

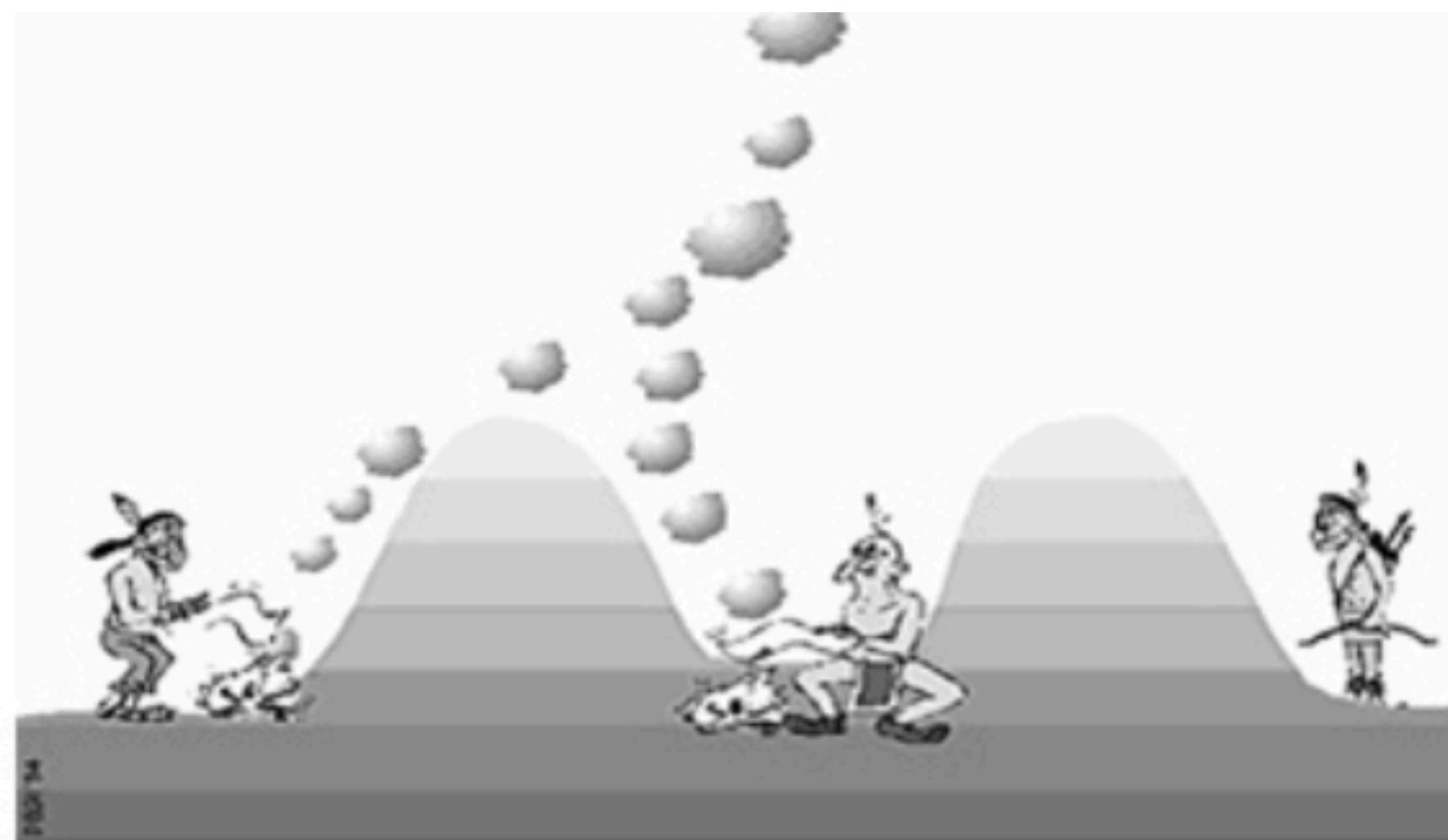


## 2. Terjaga keasliannya



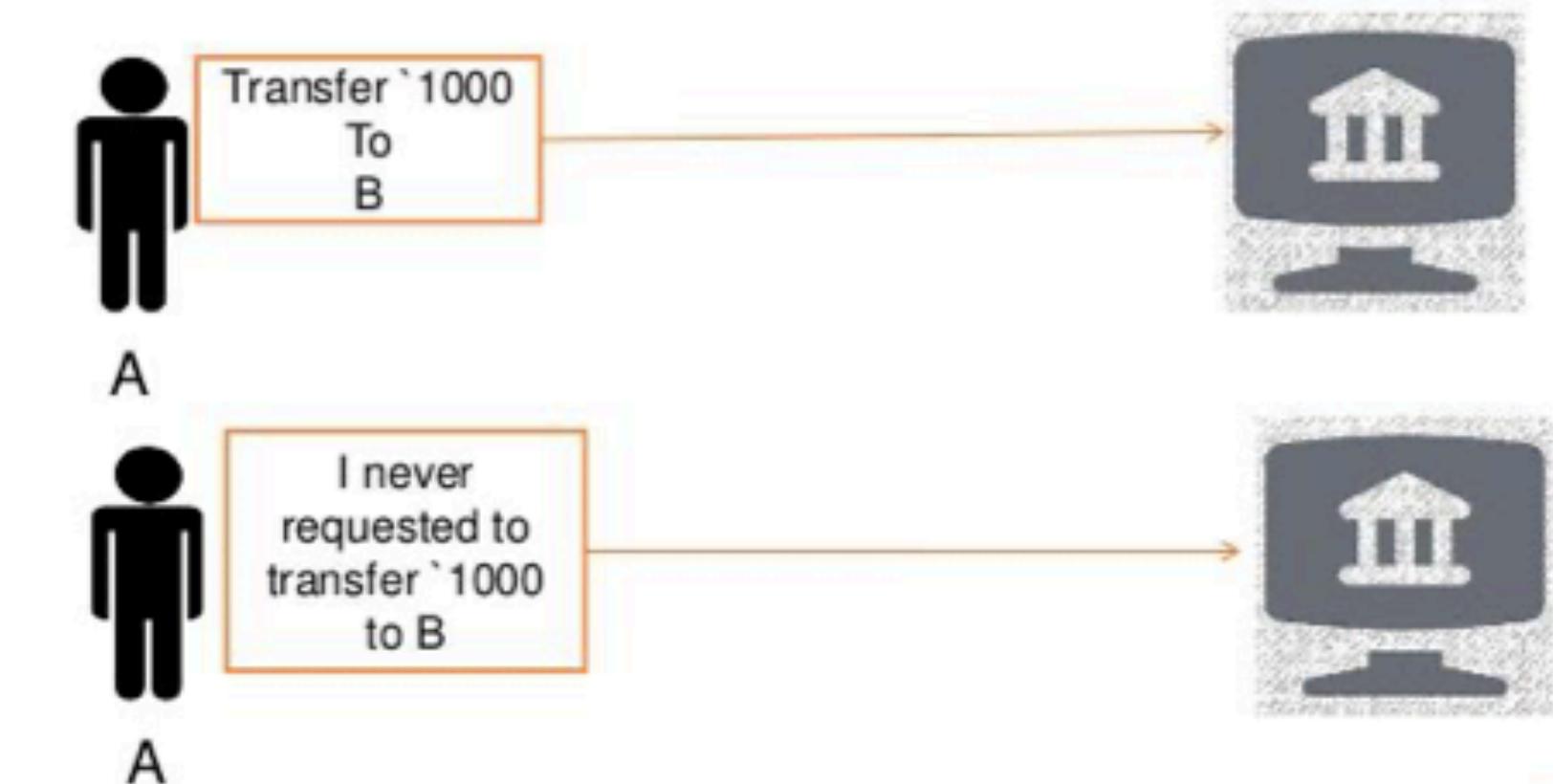
# Aman?

3. Pesan yang diterima benar-benar berasal dari pengirim yang benar



4. Pegirim pesan tidak dapat menyangkal telah mengirim pesan

## NON-REPUDIATION



# **INGAT?**

# Wikileaks



Pembocoran dokumen perang Afghanistan (Juli, 2010)

Pembocoran 400.000 dokumen perang Irak (Oktober, 2010)

- 
- 
- 



# Penyadapan di Kedubes RI di luar negeri



## Menlu: Penyadapan KBRI di Myanmar Langgar Konvensi Wina

- detikNews

Rabu, 14 Jul 2004 14:47 WIB

**Banten** - Menteri Luar Negeri Hasan Wirajuda menyesalkan terjadinya indikasi penyadapan kantor Kedutaan Besar RI di Yangon. Penyadapan dinilai melanggar konvensi Wina. Kedubes Myanmar hingga kini masih berkelit."Ada indikasi kuat mengarah kesana. Itu berdasarkan temuan tim dan hasil pemeriksaan. Atas peristiwa ini, kita sampaikan keprihatinan yang mendalam dan keras bahwa ini terjadi antar sesama anggota Asean dan jelas melanggar konvensi Wina. Dalam konvesni itu dilarang mengganggu fasilitas kedutaan karena itu menyangkut masalah kerahasiaan,".Hal ini disampaikan Menteri Luar Negeri Hasan Wirajuda usai mendampingi Presiden Megawati Soekarnoputri pada peringatan Dasawarsa Konrensi Internasional Kenendudukan dan Pembaruan di



# Penyadapan telfon Presiden SBY oleh Pemerintah Australia

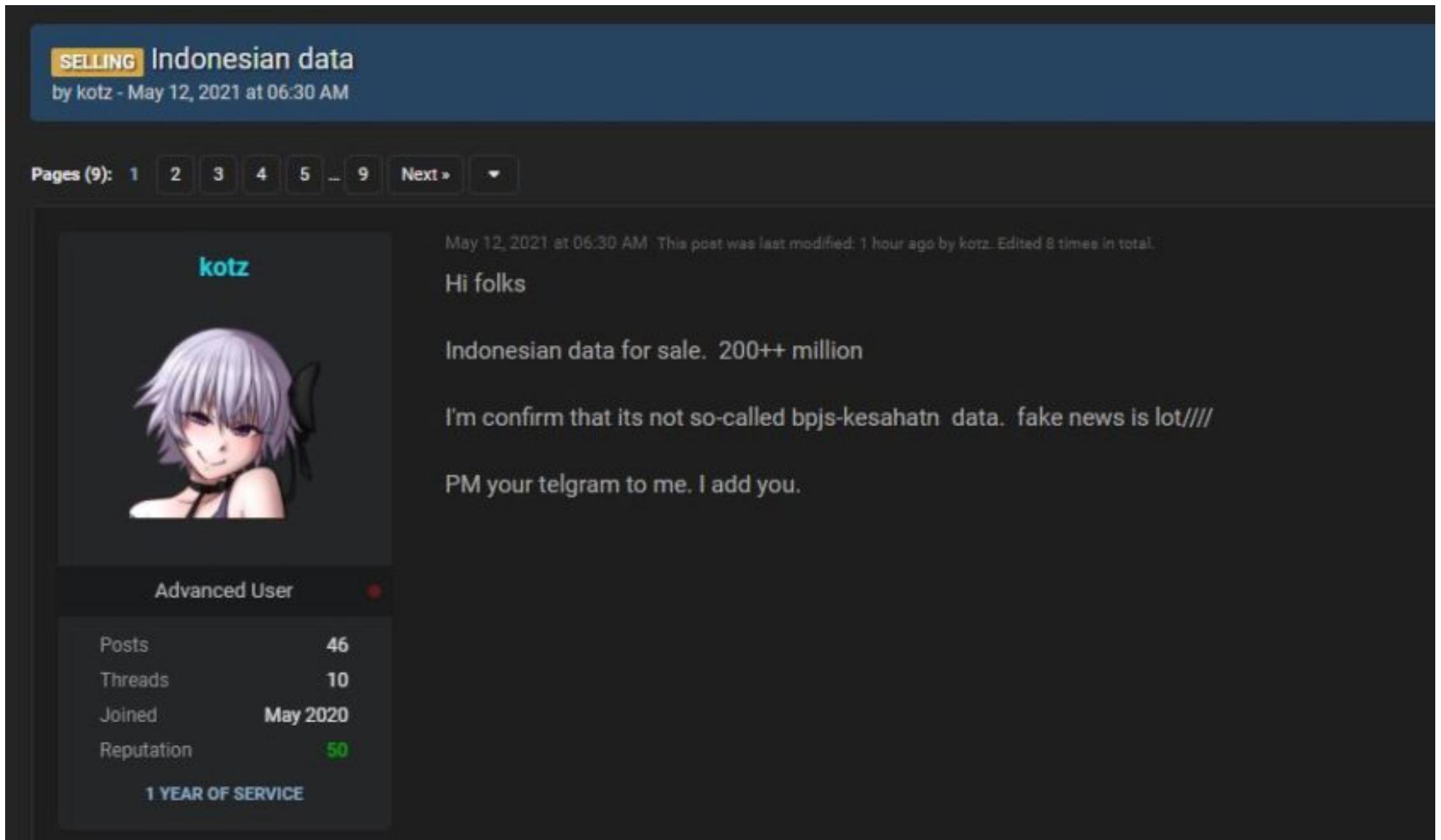
## Australia Sadap Telepon Presiden SBY, Ibu Ani dan Sejumlah Menteri!

- detikNews

Senin, 18 Nov 2013 09:59 WIB



# Kebocoran data BPJS



**SELLING** Indonesian data  
by kotz - May 12, 2021 at 06:30 AM

Pages (9): 1 2 3 4 5 ... 9 Next » ▾

May 12, 2021 at 06:30 AM This post was last modified: 1 hour ago by kotz. Edited 8 times in total.

**kotz**

Hi folks

Indonesian data for sale. 200++ million

I'm confirm that its not so-called bpjs-kesahatn data. fake news is lot///

PM your telegram to me. I add you.

Advanced User

Posts 46  
Threads 10  
Joined May 2020  
Reputation 50

1 YEAR OF SERVICE

# Kebocoran data pengguna Tokopedia

**SELLING** Tokopedia 91 million users for sale  
by whysodank · Yesterday at 08:40 PM

Yesterday at 08:40 PM · This post was last modified: 10 hours ago by whysodank. Edited 1 time in total.

Hello. So the full tokopedia is for sale on empire market:  
<http://gshgz5z12blfqbltnbzpxn6icu3iue74...49/1008904>  
Feel free to PM me here too.  
I already post some samples:  
<https://raiddforums.com/Thread-UPDATE-Exc...lion-users>

★ whysodank



VIP User

**VIP**

Posts	6
Threads	3
Joined	Apr 2020
Reputation	20

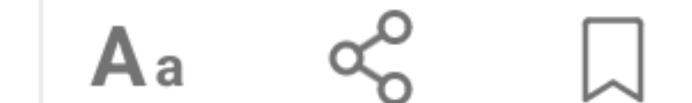
★

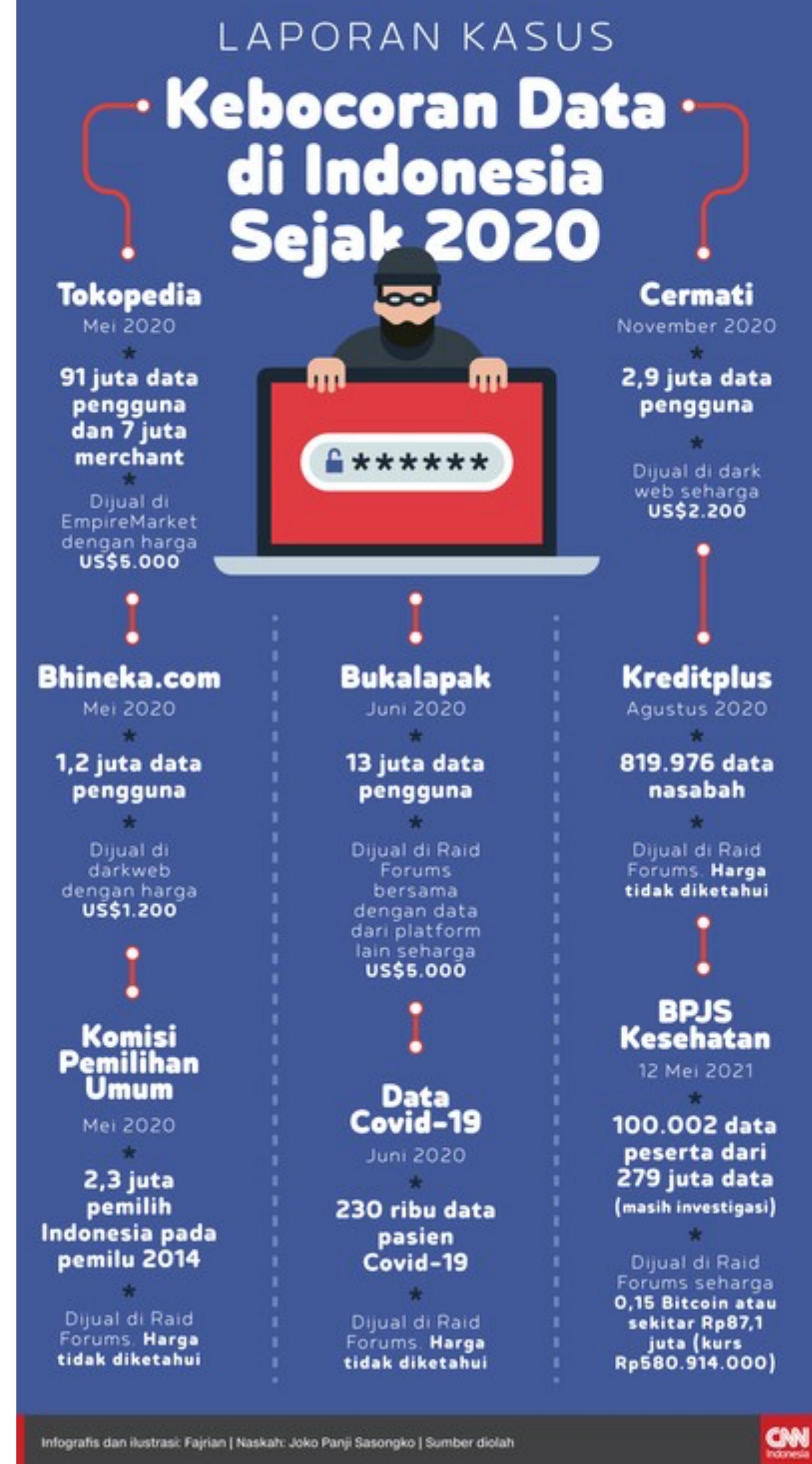
# Kebocoran data di kemenhan

## **Situs Web Kemenhan Dibobol, Pakar Siber: Data Pribadi 667 User dan 37 Karyawan Bocor**

Pakar keamanan siber dari CISSReC merespons adanya serangan siber yang menargetkan situs web Kementerian Pertahanan (Kemenhan).

2 November 2023 | 22.00 WIB





Kasus-kasus seperti:

- Kebocoran data,
- pencurian data,
- pengaksesan data secara ilegal

...

Menunjukkan pentingnya **kriptografi** menjaga keamanan data dan informasi

**Q:** What can a “bad guy” do?

**A:** a lot!

- **eavesdrop:** intercept messages
- actively **insert** messages into connection
- **impersonation:** can fake (spoof) source address in packet (or any field in packet)
- **hijacking:** “take over” ongoing connection by removing sender or receiver, inserting himself in place
- **denial of service:** prevent service from being used by others (e.g., by overloading resources)

Sumber: Chapter 8, Network Security

!

**Cipherteks:** pesan yang telah disandikan sehingga tidak bermakna lagi.

Tujuan: agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.

Nama lain: **criptogram**

**Plainteks:** culik anak itu jam 11 siang

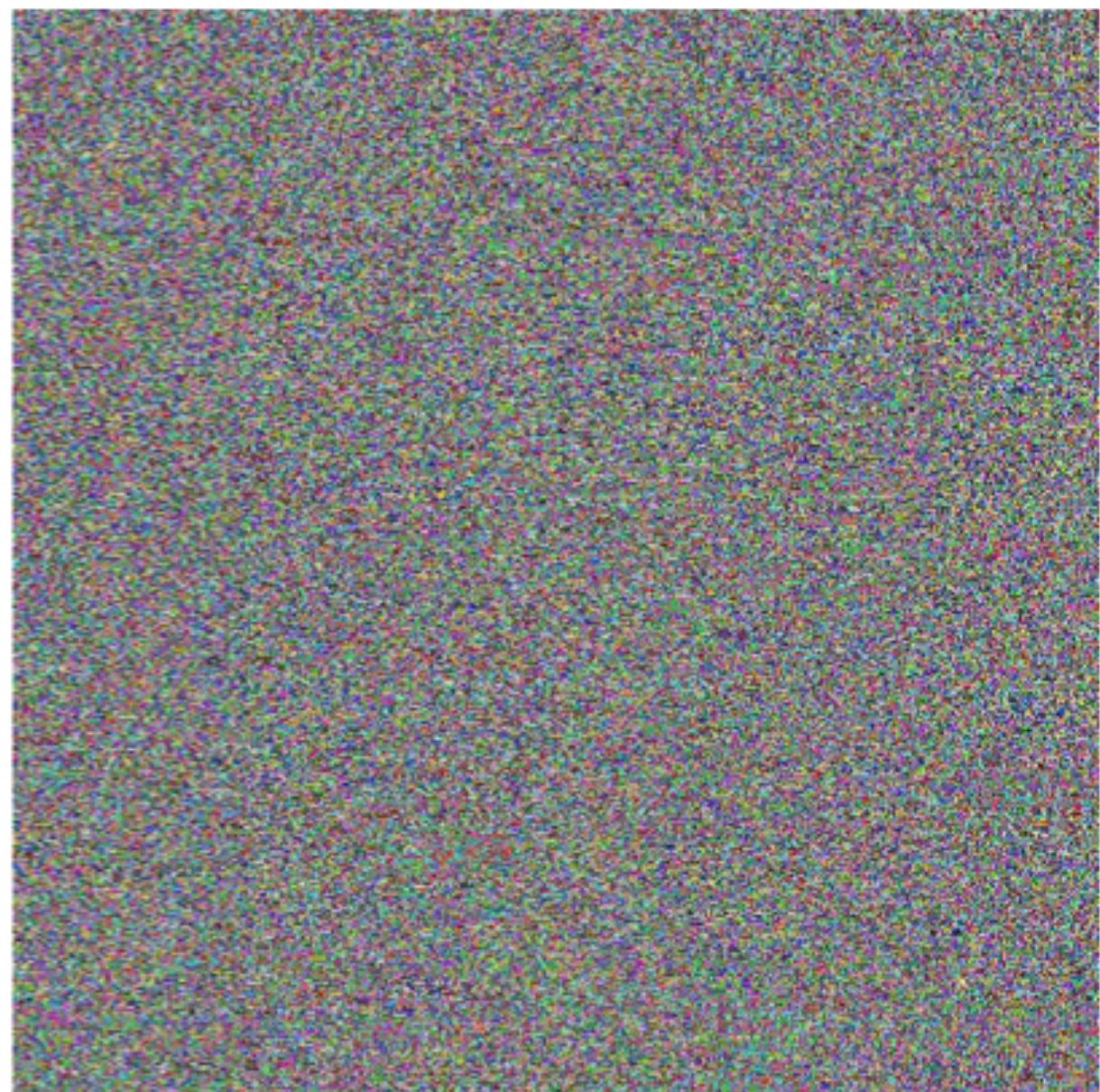
**Cipherteks:** t^\$gfUi89rewoFpfldWqLMp [uTcxZ

**Kriptogram:** t^\$gfU, i89rewo, FpfldWqLM, p [uTcxZ

!



Plain-image



Cipher-image

!



Plain-video

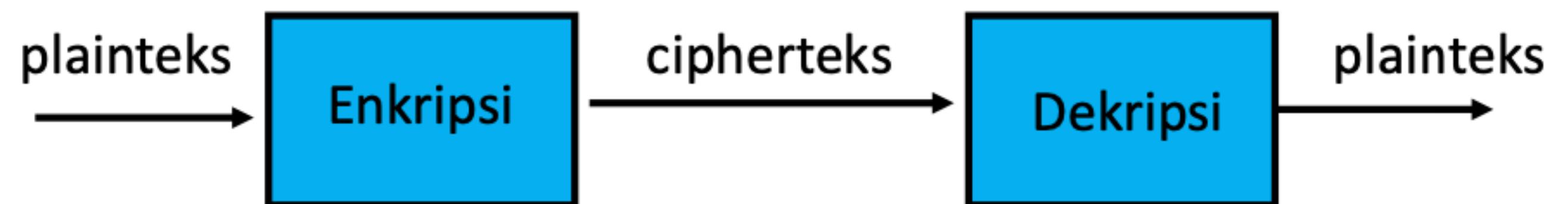


Cipher-video

!

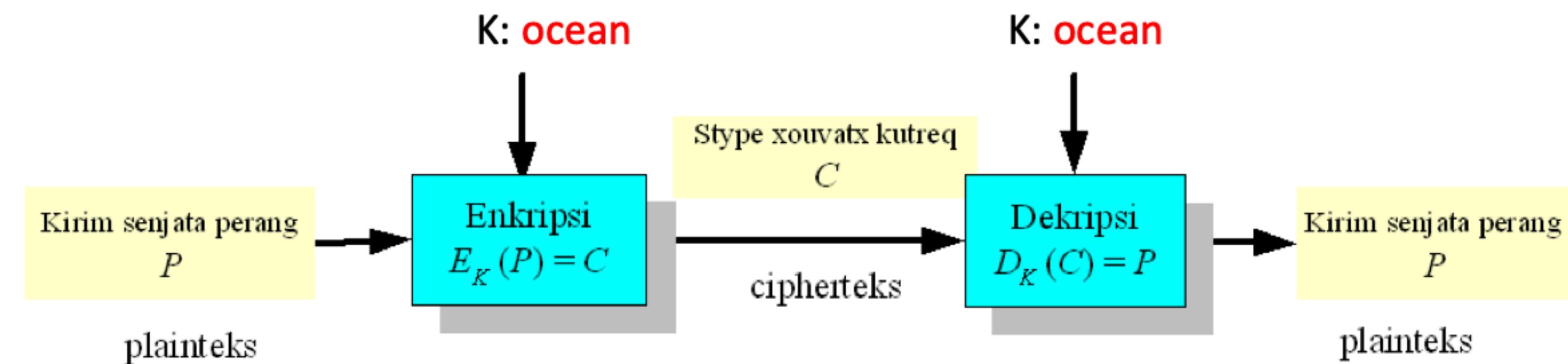
**Enkripsi:** proses menyandikan plainteks menjadi chiperteks

**Dekripsi:** proses mengembalikan teks menjadi plainteks semula



!

**Kunci:** parameter yang digunakan di dalam enkripsi dan deskripsi  
**Simbok:** K (K dapat berupa integer, string, alphanumeric, dsb)



!

**Kriptanalisis:** ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan.

Kriptanalisis dikemukakan pertama kali oleh seorang ilmuan Arab pada Abad IX bernama Abu Yusuf Yaqub Ibnu Ishaq Ibnu As-Sabbah Ibnu ‘Omran Ibnu Ismail Al-Kindi, atau yang lebih dikenal Al-Kindi



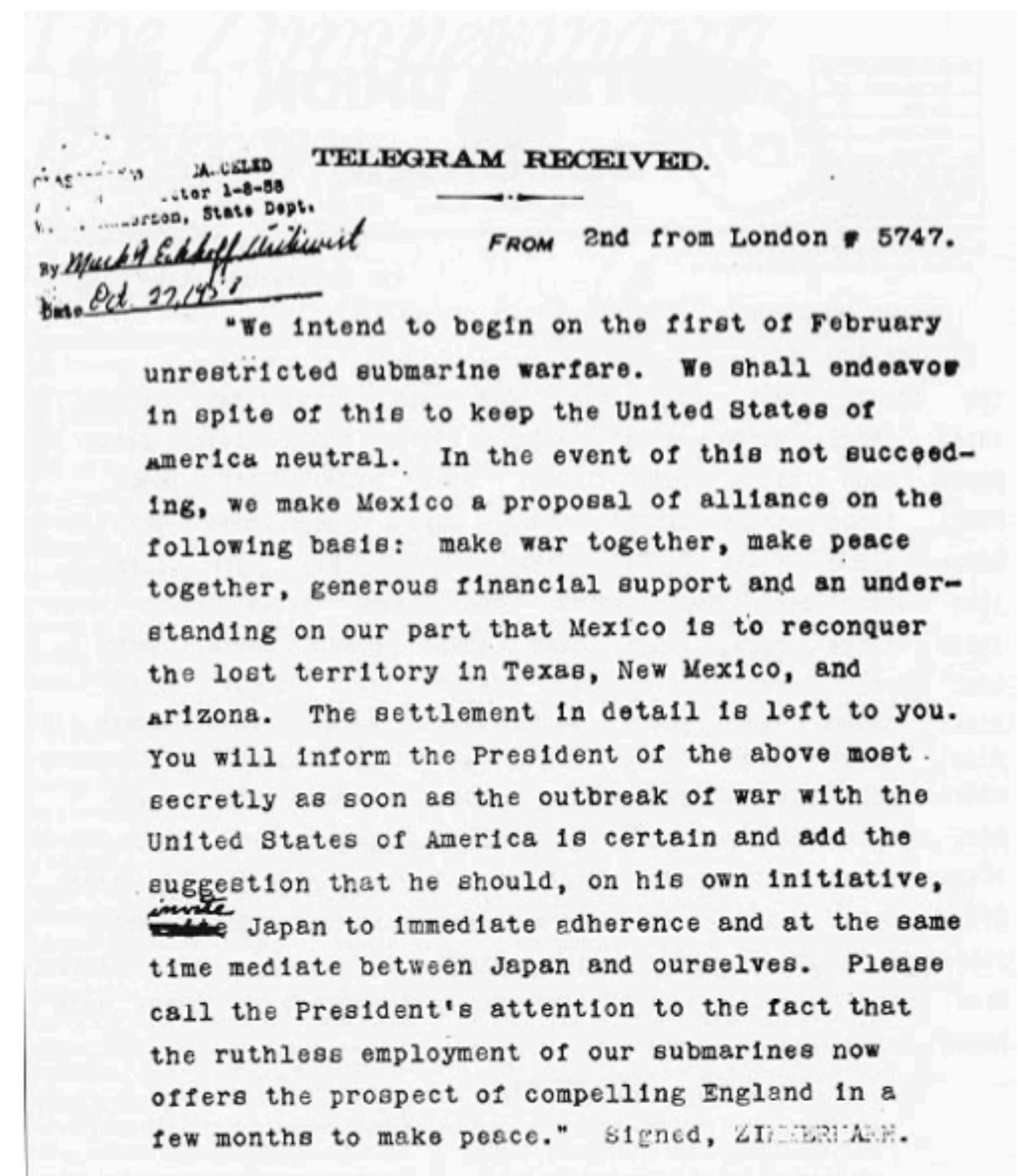
ذات الرؤوس والذهب، نصفه في كل يوم، العترة أعرق من رأى، والباقي على عمار،  
ومن ملائكة الله، يحيى في منطمه طلاق، وشأنه علم، بما يحمله الظماء، وسبعين طلاقاً  
عما يعسر، لما يطرد الطير، يحصل به ذلك، فور العفة، والأمسى، يعلمونه ويسخنه؛  
بل حكمه، وسر دعهم، والليل يصعبه، الليل يصعبه، والربيع المحرر، يصعبه  
من الأحشاء، لهم بايو، ونقاء، ازدواج ذكره، وإنك، والركب طبعاً، السرور ملنا، السماوة، الراية  
رس، سر الأحشاء، ويلهم، قلبي، والرحم، والمعن، وجهه، ولهم سر الصار، يلهم، يصعبه  
أسمر، السفاف، ما يلهم، المريء، ويعسل، الطير بالصوت، الطير، النفس، ص

مرادله - ولله الحمد والصلوة والسلام على سيدنا محمد وآله وآل بيته

Halaman pertama buku Al-Kindi,  
*Manuscript for the Deciphering Cryptographic*

!

# Sejarah kriptanalisis mencatat hasil gemilang seperti pemecahan Telegram Zimmerman yang membawa Amerika Serikat ke Perang Dunia I



Telegram Zimmerman yang sudah berhasil didekripsi (Sumber: Wikipedia.org)

# **TUGAS**

!

**Buat dua kelompok:**

- 1. Old Cryptography**
- 2. Modern Cryptography**

**SELAMAT  
BELAJAR**