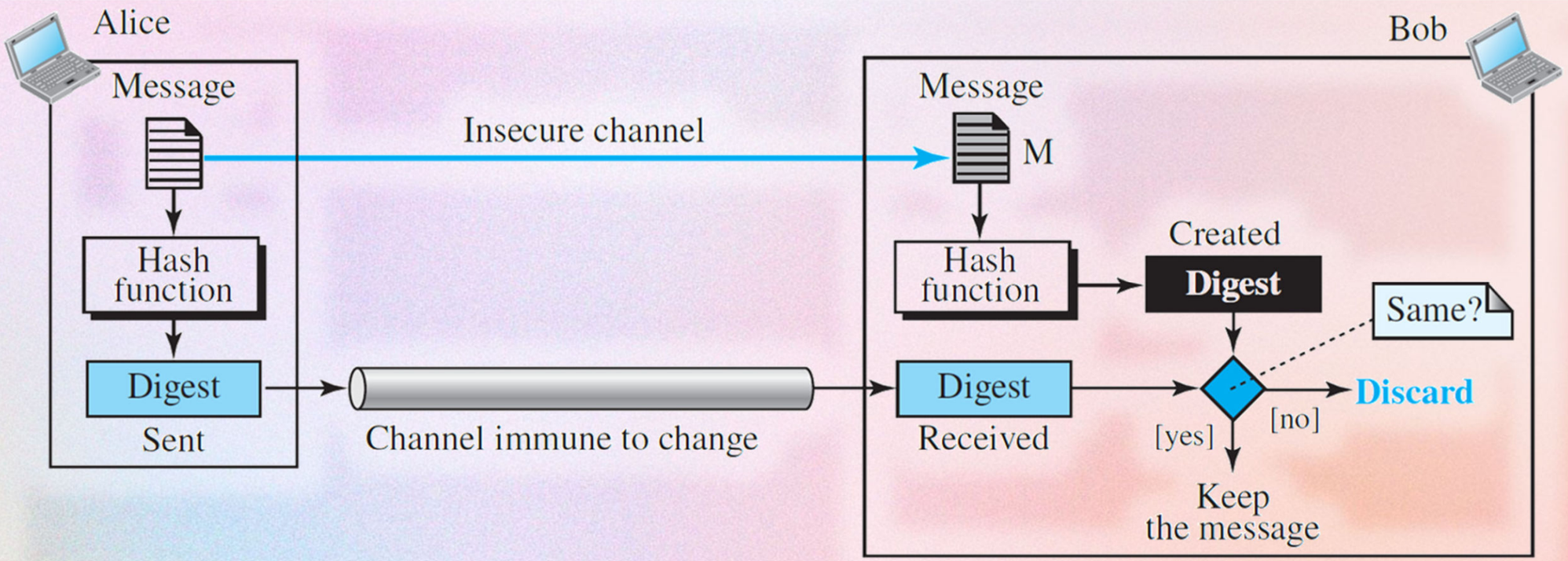
DIGITAL SIGNATURES

CRYPTOGRAPHIC HASH FUNCTIONS

A cryptographic hash function ***converts any message into a fixed-length n-bit string*** *called a* ***digest.***



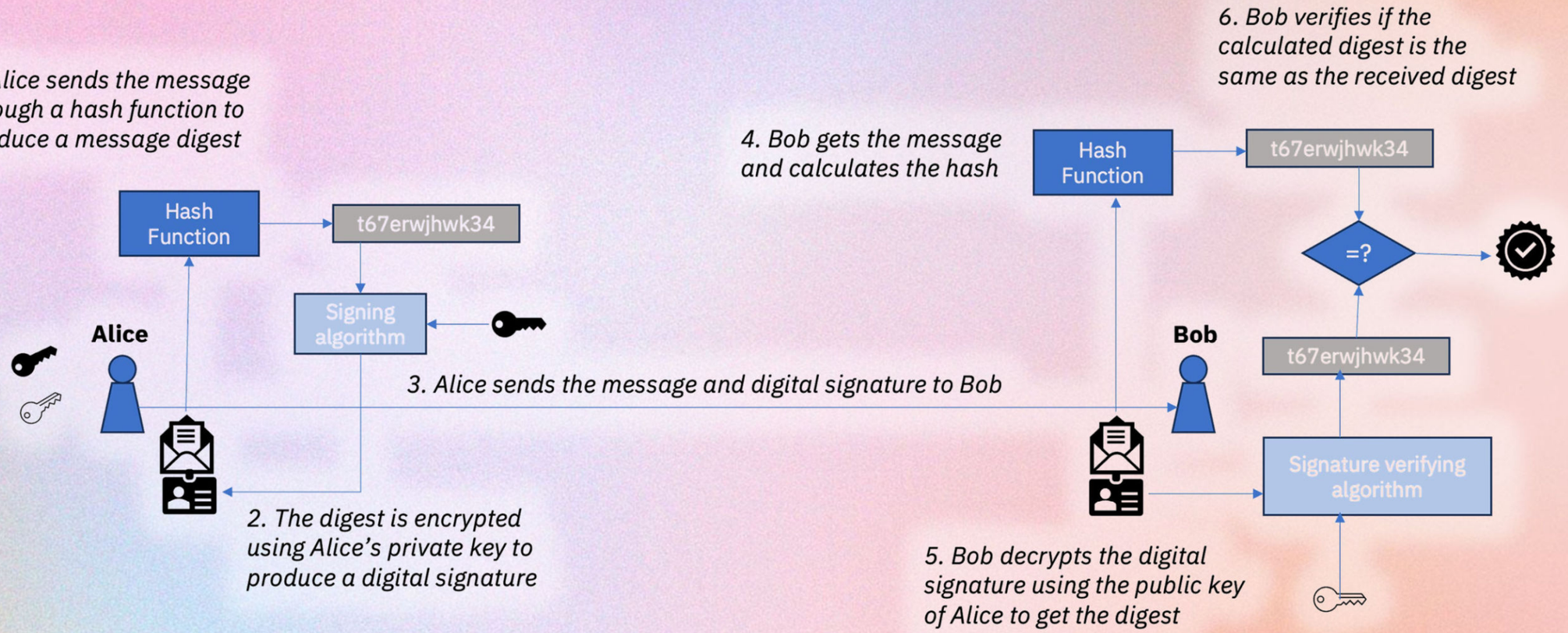
Data Communications And Networking, Behrouz A Forouzan

https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography

COMMONLY USED CHFs

Hash Function	Output Length (bits)	Common Applications
MD5	128	File integrity checking, older systems, non-crypto uses
SHA-1	160	Legacy systems, Git for version control
SHA-256	256	Cryptocurrency (Bitcoin), digital signatures, certificates
SHA-3	Variable (up to 512)	Various cryptographic applications, successor to SHA-2
Blake2	Variable (up to 512)	Cryptography, replacing MD5/SHA-1 in some systems
Blake3	Variable (up to 256)	Cryptography, file hashing, data integrity

DIGITAL SIGNATURES



FOR THIS UNIT...

01 WHAT IS A DIGITAL SIGNATURE?

02 PERSONAL VS. DIGITAL SIGNATURE

03 PROCESS

04 CREATING A DIGITAL SIGNATURE

FOR THIS UNIT...

05 DIGITAL SIGNATURE ASSURANCES

01

WHAT IS A DIGITAL SIGNATURE?

Content Curated by Pollux M. Rey

More and more people and organizations are using **digital documents instead of paper documents** to conduct day-to-day transactions.

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-3186cd15-e7ac-4a16-8597-22bd163e8e96

Digital signatures support this change by providing assurances about the **validity and authenticity of a digital document.**

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-3186cd15-e7ac-4a16-8597-22bd163e8e96

A **digital signature** on an electronic document or other object is **created by using a form of cryptography** and is **equivalent to a personal signature on a written document.**

Content Curated by Pollux M. Rey

https://www.ibm.com/docs/cn/i/7.5?topic=concepts-digital-signatures

02

PERSONAL VS. DIGITAL SIGNATURE

Content Curated by Pollux M. Rey

CONVENTIONAL VS. DIGITAL SIGNATURES

Characteristics	Conventional Signature	Digital Signature
Inclusion	Physically applied to the document itself	Added as a separate data
Verification Method	Checks the document's signature against a stored sample	Needs to apply a verification technique to the message and the signature
Relationship	One-to-many	One-to-one
Duplicity	Copies of the signed document can be distinguished from the original	Cannot be distinguished from copies unless they're timestamped

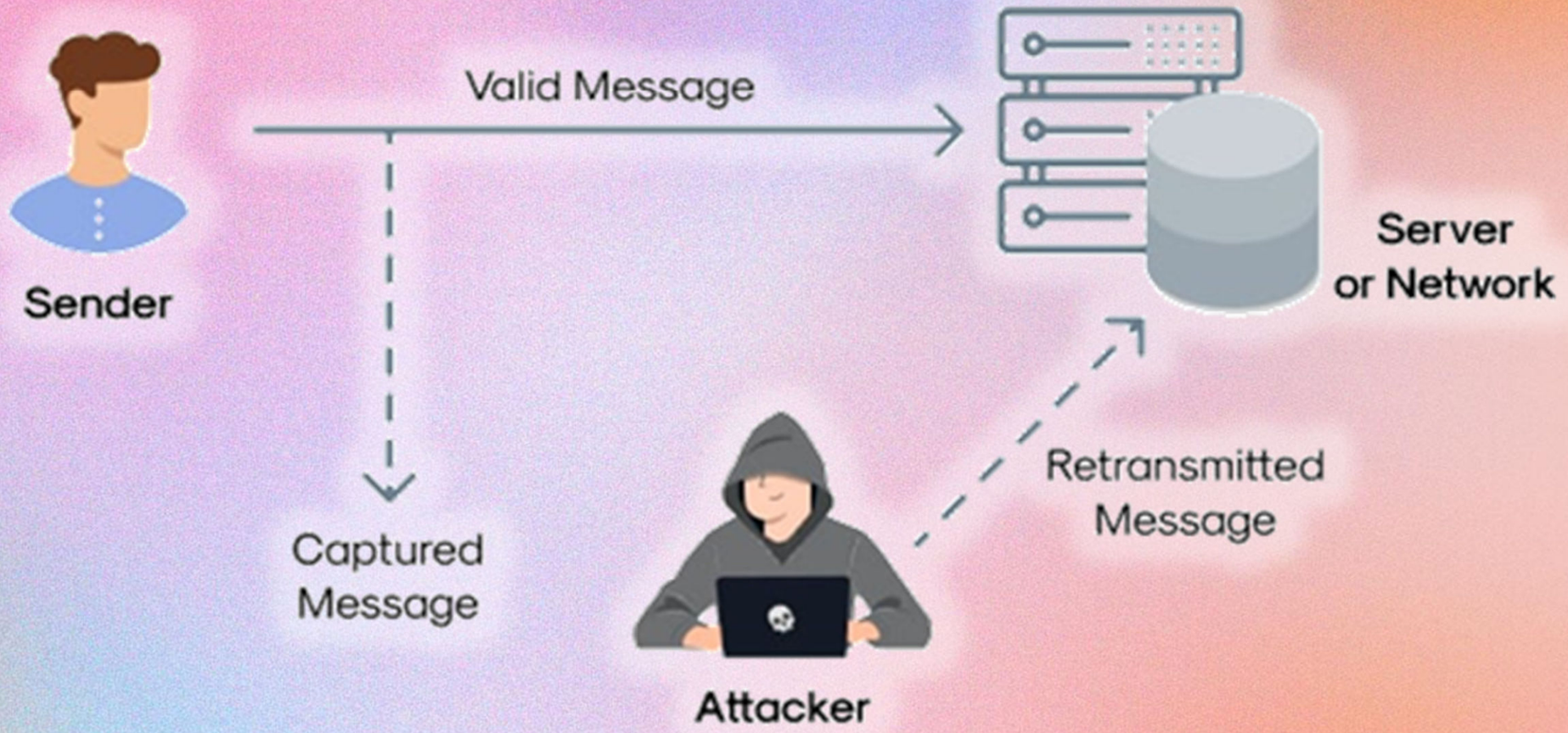
Data Communications and Networking, Behrouz A Forouzan

CONVENTIONAL VS. DIGITAL SIGNATURES

Characteristics	Conventional Signature	Digital Signature
Inclusion	Physically applied to the document itself	Added as a separate data
Verification Method	Checks the document's signature against a stored sample	Needs to apply a verification technique to the message and the signature
Relationship	One-to-many	One-to-one
Duplicity	Copies of the signed document can be distinguished from the original	**Cannot be distinguished from copies unless they're timestamped**

Data Communications and Networking, Behrouz A Forouzan

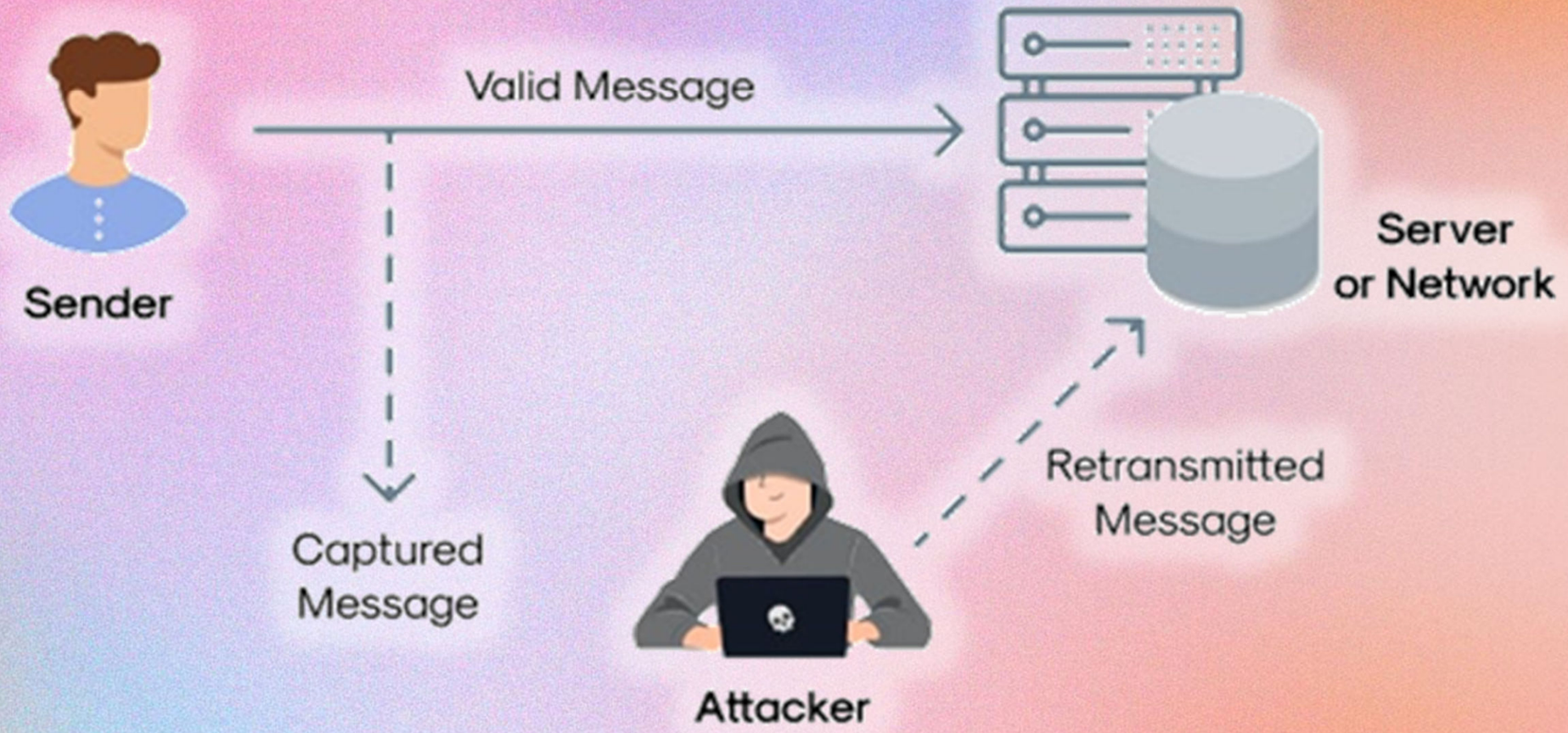
DUPLICITY OF A DIGITAL SIGNATURE



Bob (sender) sends a withdrawal request to the server.

https://www.wallarm.com/what/replay-attacks

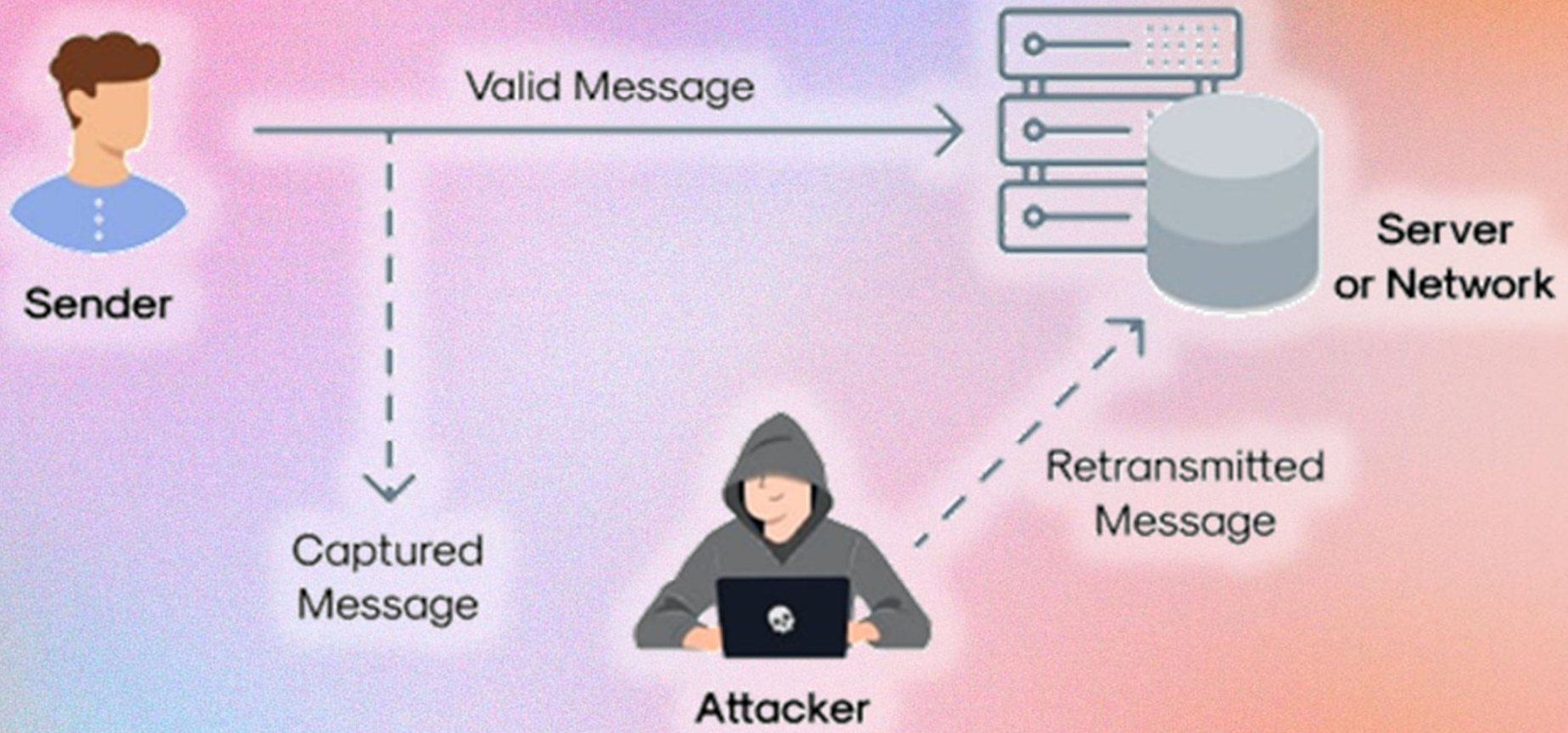
DUPLICITY OF A DIGITAL SIGNATURE



Eve (attacker) intercepts and later replays Bob's message.

https://www.wallarm.com/what/replay-attacks

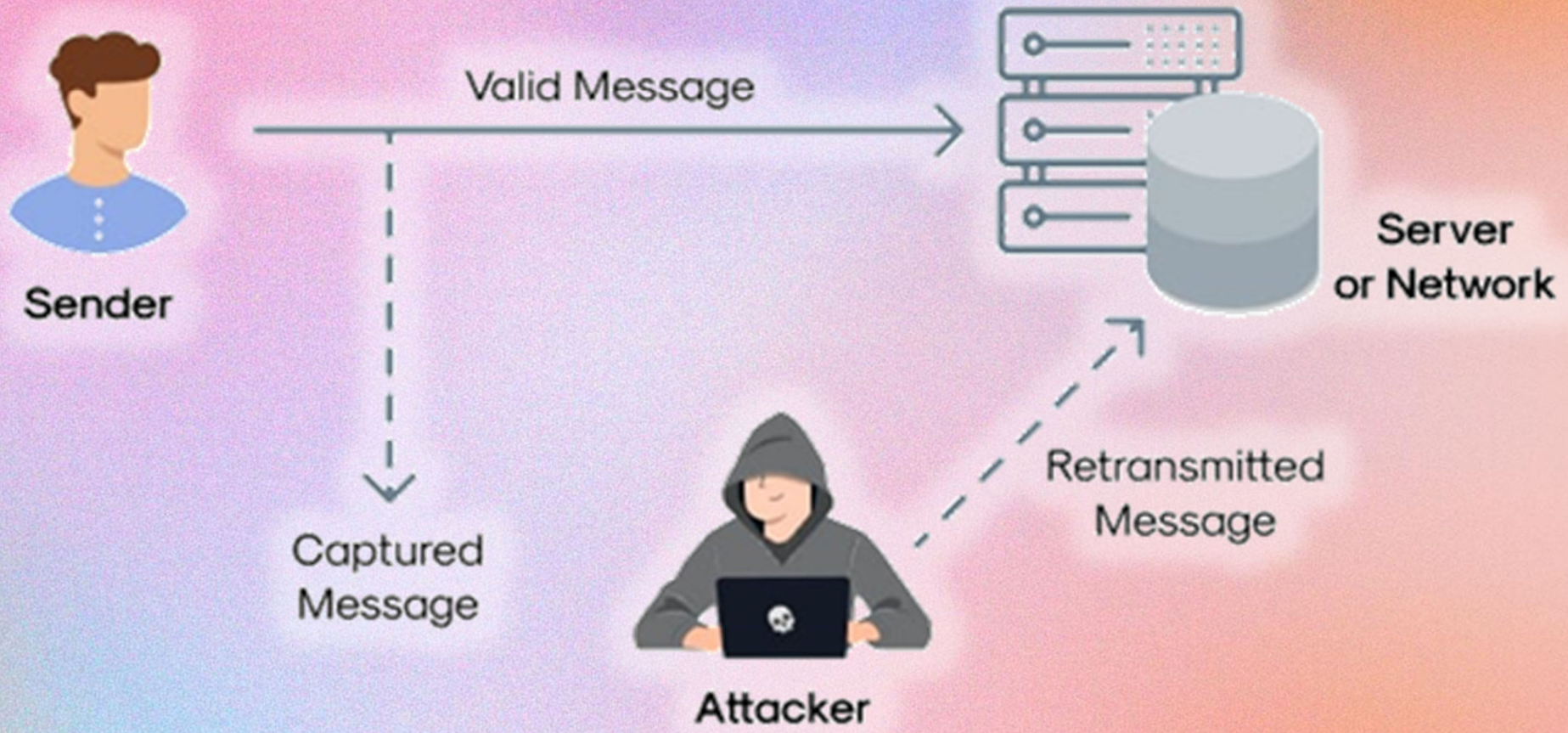
DUPLICITY OF A DIGITAL SIGNATURE



Without a timestamp, the server might process the replayed message as a new request.

https://www.wallarm.com/what/replay-attacks

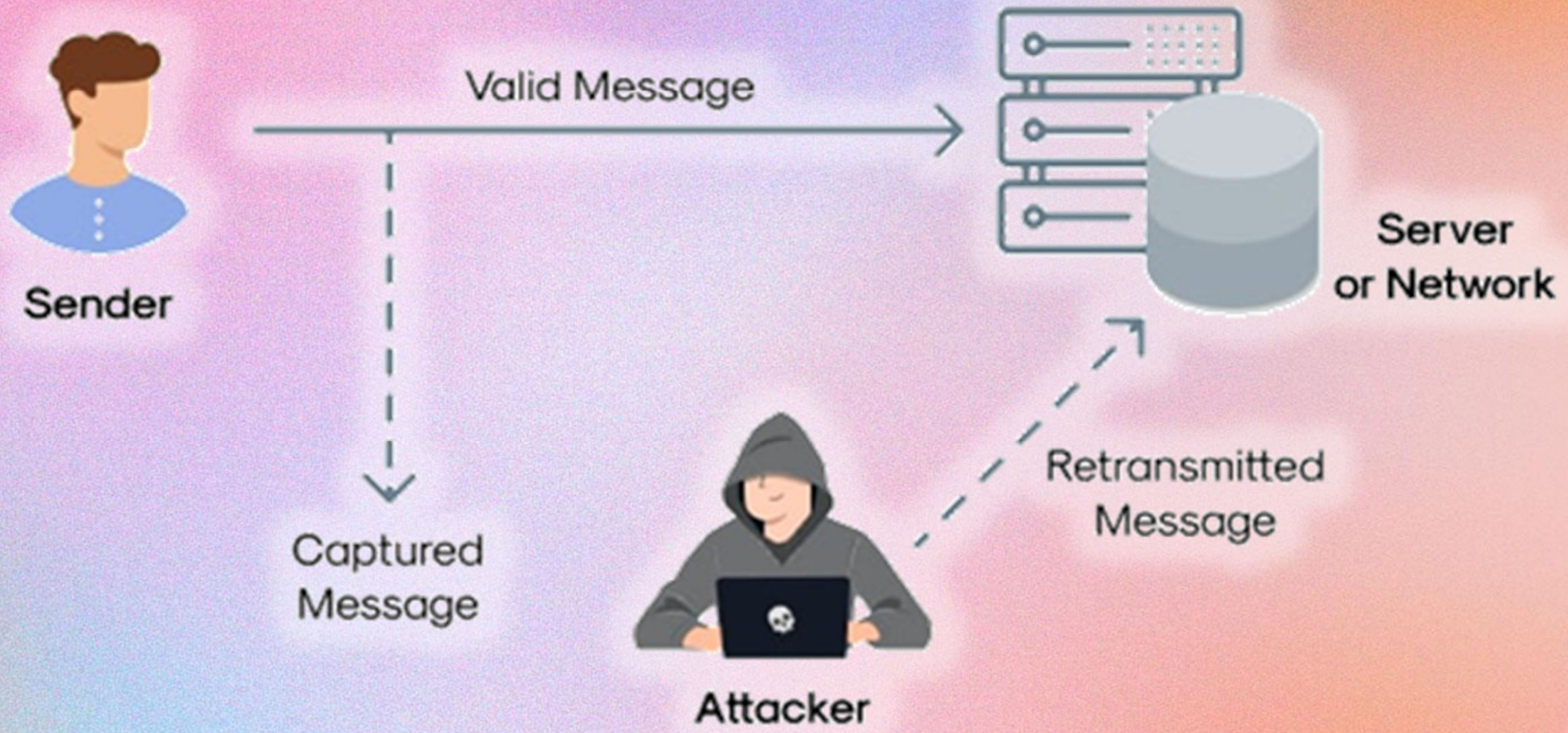
DUPLICITY OF A DIGITAL SIGNATURE



A timestamp helps the server detect and ignore duplicate requests.

https://www.wallarm.com/what/replay-attacks

REPLAY ATTACK



A timestamp helps the server detect and ignore duplicate requests.

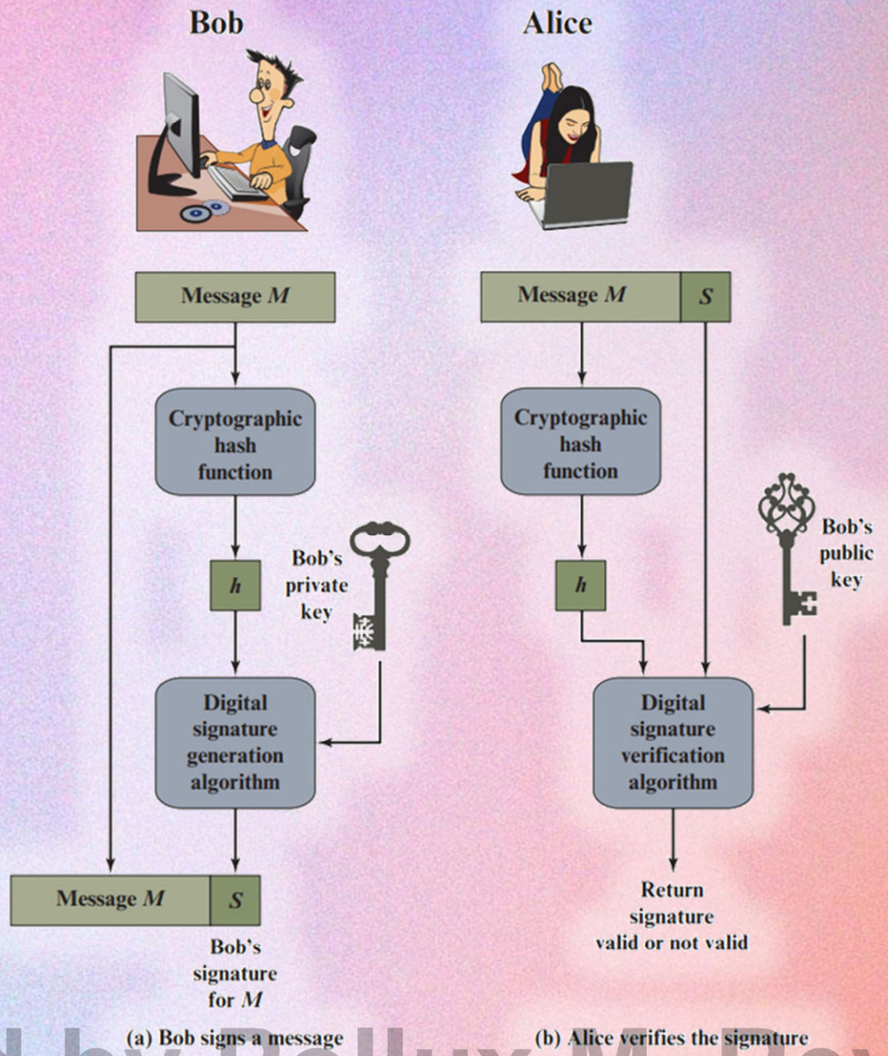
https://www.wallarm.com/what/replay-attacks

03

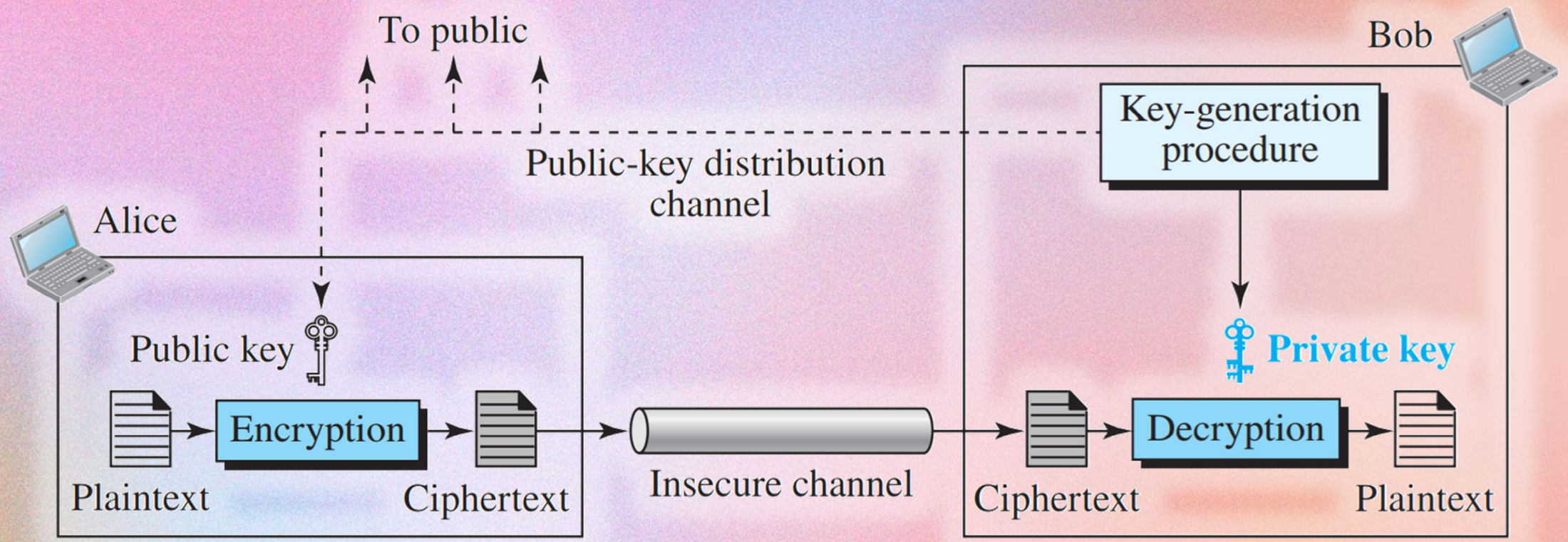
PROCESS OF A DIGITAL SIGNATURE

Content Curated by Pollux M. Rey

PROCESS OF A DIGITAL SIGNATURE



ASYMMETRIC-KEY CIPHER



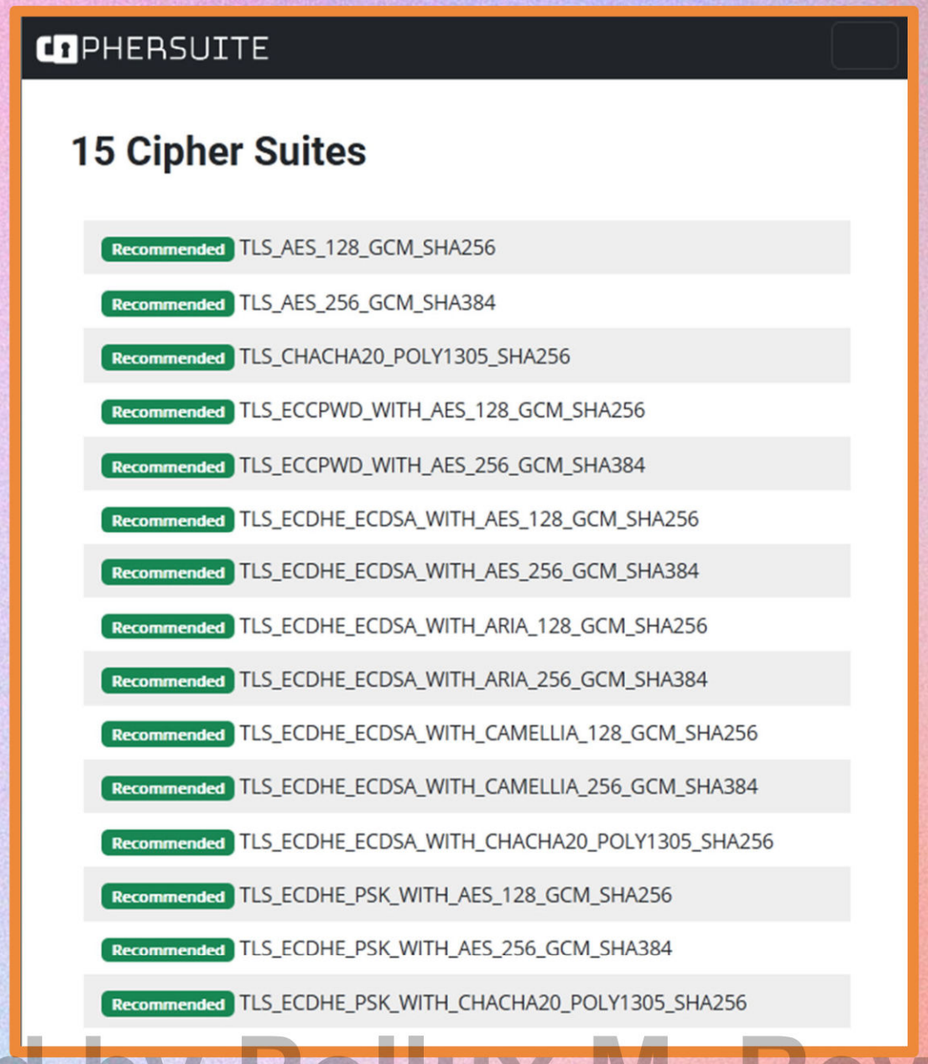
SOME DIGITAL SIGNATURE ALGORITHMS

RSA

Digital Signature Algorithm (DSA)

Elliptic Curve Digital Signature Algorithm (ECDSA)

SOME DIGITAL SIGNATURE ALGORITHMS



04

CREATING A DIGITAL SIGNATURE

Content Curated by Pollux M. Rey

To create a digital signature, **you need a digital certificate**, which proves identity.

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-3186cd15-e7ac-4a16-8597-22bd163e8e96

When you send a digitally-signed document, **you also send your certificate and public key.**

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-3186cd15-e7ac-4a16-8597-22bd163e8e96

Certificates are issued by a **certification authority (CA)**.

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-3186cd15-e7ac-4a16-8597-22bd163e8e96

A **certification authority (CA) issues digital certificates, signs certificates** to verify their validity and tracks which certificates have been revoked or have expired.

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96

JUAN DELA CRUZ, M.D., DPBA, DPBPM
Anesthesiology
Pain Medicine and Palliative Care

JUAN DELA CRUZ MEDICAL CENTER
3/F PCAS Building
#10 ABC St,, Greenhills, San Juan
Mon to Fri 8am-12nn / 1pm-4pm
BY APPOINTMENT

Trunk Line:
123-4567 Loc. 5300 to 5305
Direct Line: 123-4567
Mobile: 0912-345-5678
juandelacruz@abc.ph

Patient's Name: _____ **Age:**_____ **_Sex:**_____

Address:_____ **Date:** _____

Rx

Juan Dela Cruz M.D., DPBA, DPBPM
Lic No. _____
S2. No. _____
Date of Issue _____
Date of Expiry _____
PTR No. _____

Make sure your documents and eSignatures are kept safe and secure.

GET YOUR DIGITAL SIGNATURE AND DIGITAL CERTIFICATE FOR FREE

SWIPE LEFT TO APPLY

DICT LUZON CLUSTER 3

GET YOUR DIGITAL SIGNATURE AND DIGITAL CERTIFICATE NOW WITH PNPKI!

WHO CAN AVAIL:

MIMAROPA and Bicol Regions:

- Government agencies and personnel
- Private individuals
- Government computers, servers and machines

FEATURES:

- Authentication in Web applications
- Electronic Documents and Forms Signing
- Email and Instant Messaging

REQUIREMENTS:

- Duly accomplished application form
  download at: https://bit.ly/PNPKform
- Birth Certificate or valid Philippine Passport
- 1 passport size photo taken within the last six months
- Unified Multi-Purpose Identification (UMID) compliant card (Photocopy)

SUBMIT E-COPY OF THE ABOVE REQUIREMENTS AT LC3.SUPPORT.PNPKI@DICT.GOV.PH

DICT DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY LUZON CLUSTER 3

PHILIPPINE NATIONAL PKI

For more info visit :
https://dict.gov.ph/pnpki/
E-mail: **lc3.support.pnpki@dict.gov.ph**
FB page: **facebook.com/dictlc3/**

Content Curated by Pollux M. Rey

https://dict.gov.ph/pnpki

05

DIGITAL SIGNATURE ASSURANCES

Content Curated by Pollux M. Rey

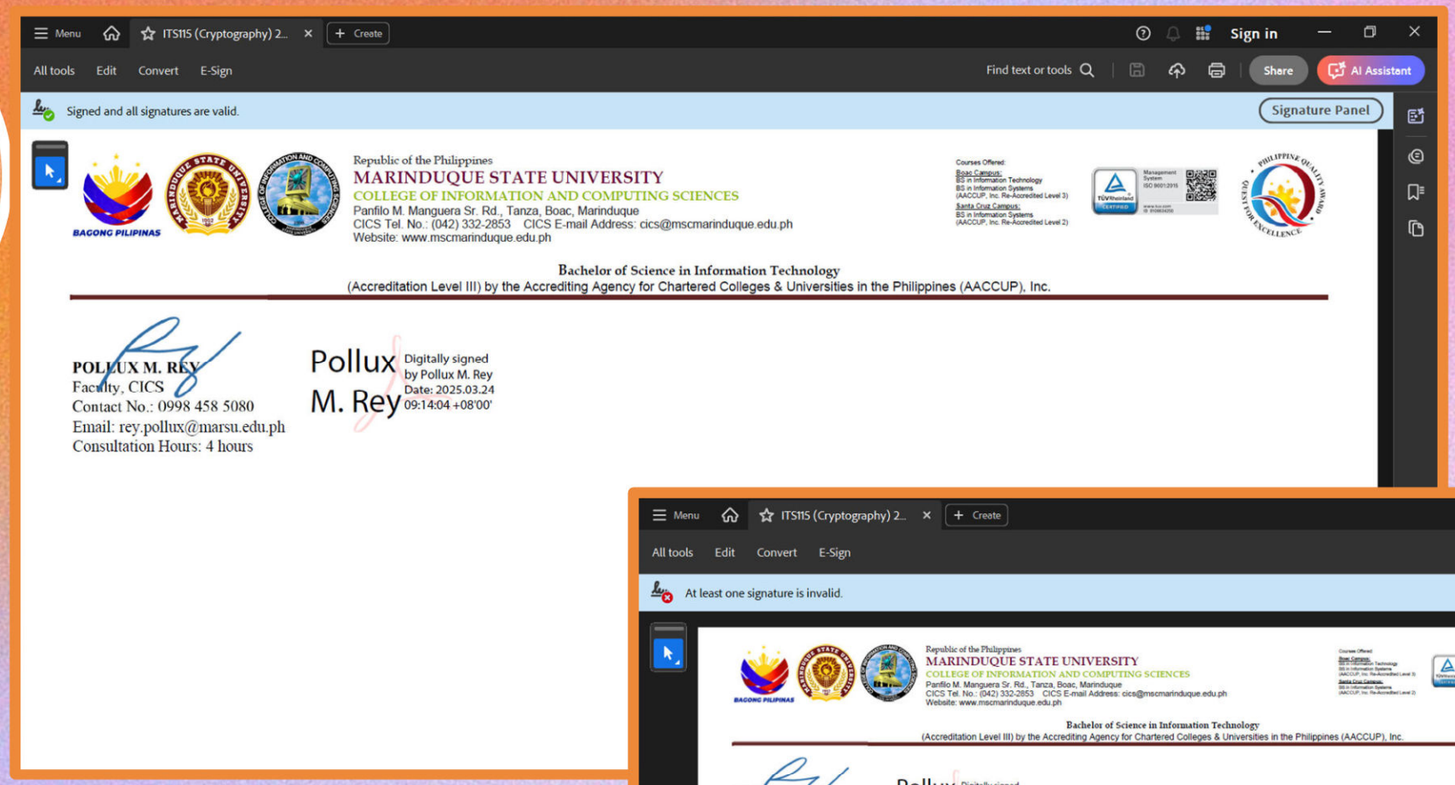
DIGITAL SIGNATURE ASSURANCES

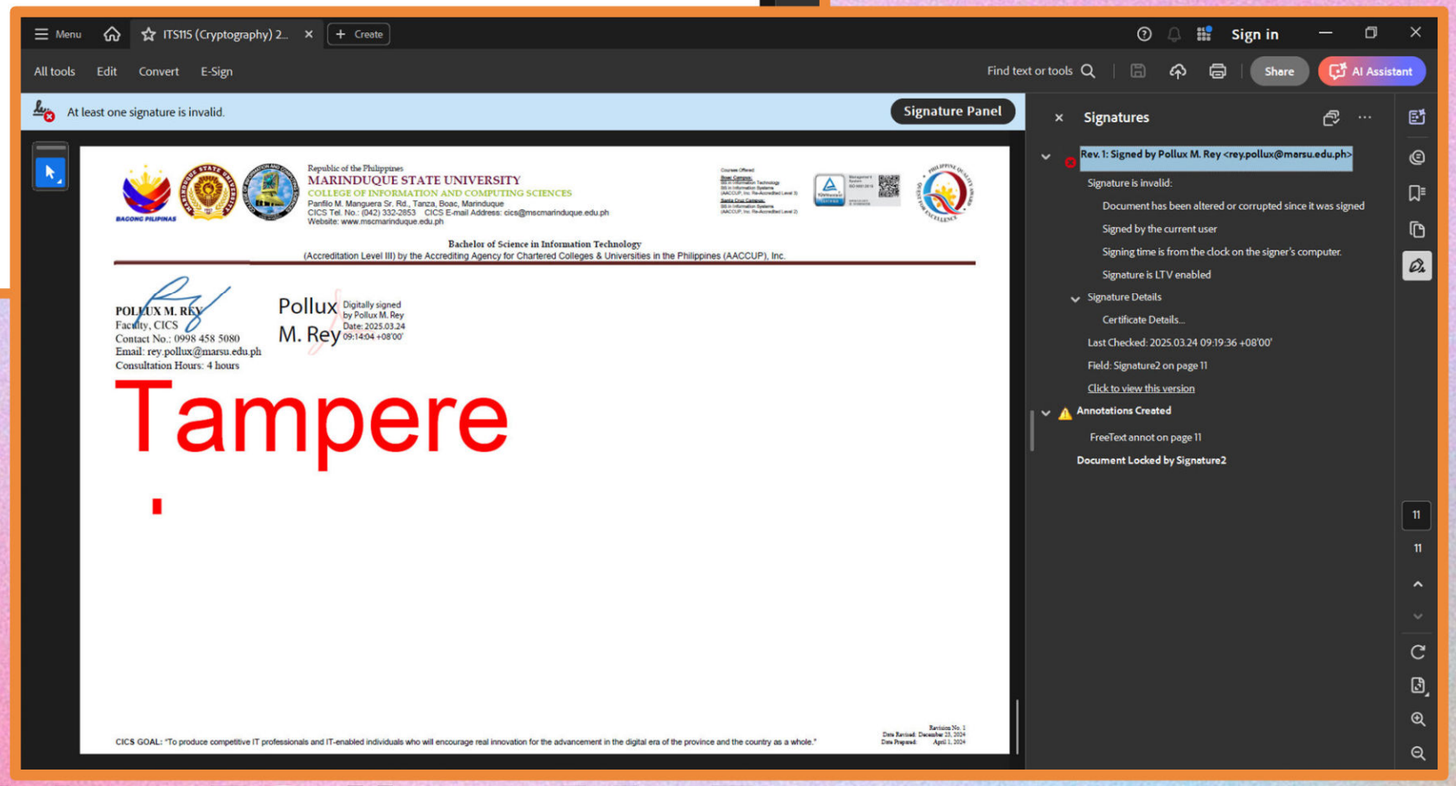
Security Assurance	Description
Authenticity	The signer is confirmed as the signer.
Integrity	The content has not been changed or tampered with since it was digitally signed.
Non-repudiation	Proves to all parties the origin of the signed content. Repudiation refers to the act of a signer denying any association with the signed content.

DIGITAL SIGNATURE ASSURANCES

To make these assurances, the content creator must digitally sign the content by using a signature that satisfies the following criteria:

1. The digital signature is valid.
2. The certificate associated with the digital signature is current (not expired).
3. The signing person or organization, known as the publisher, is trusted.
4. The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA).





THANK YOU!

Content Curated by Pollux M. Rey