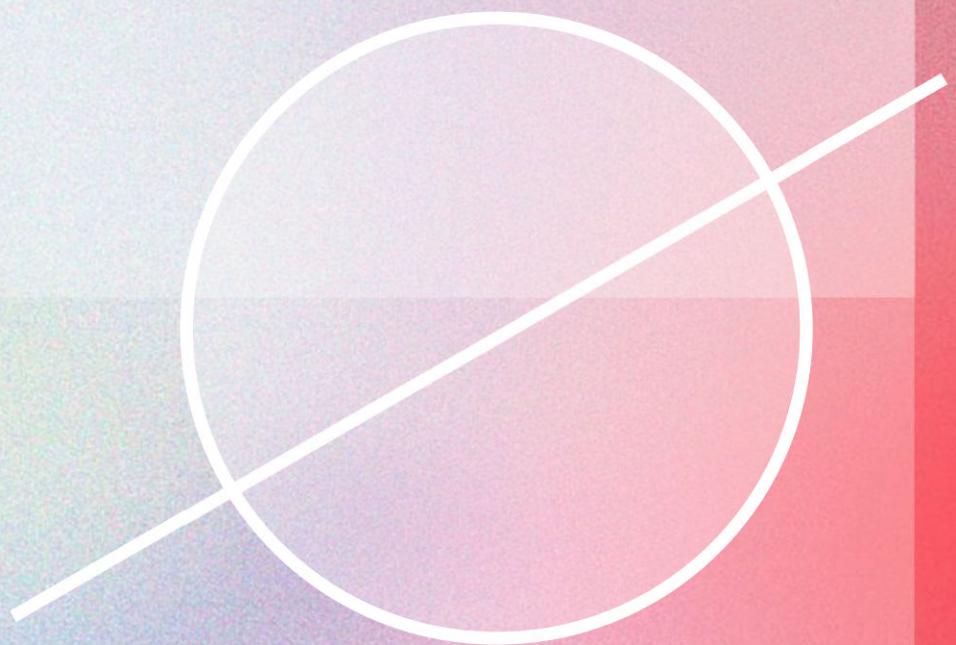


DIGITAL SIGNATURES

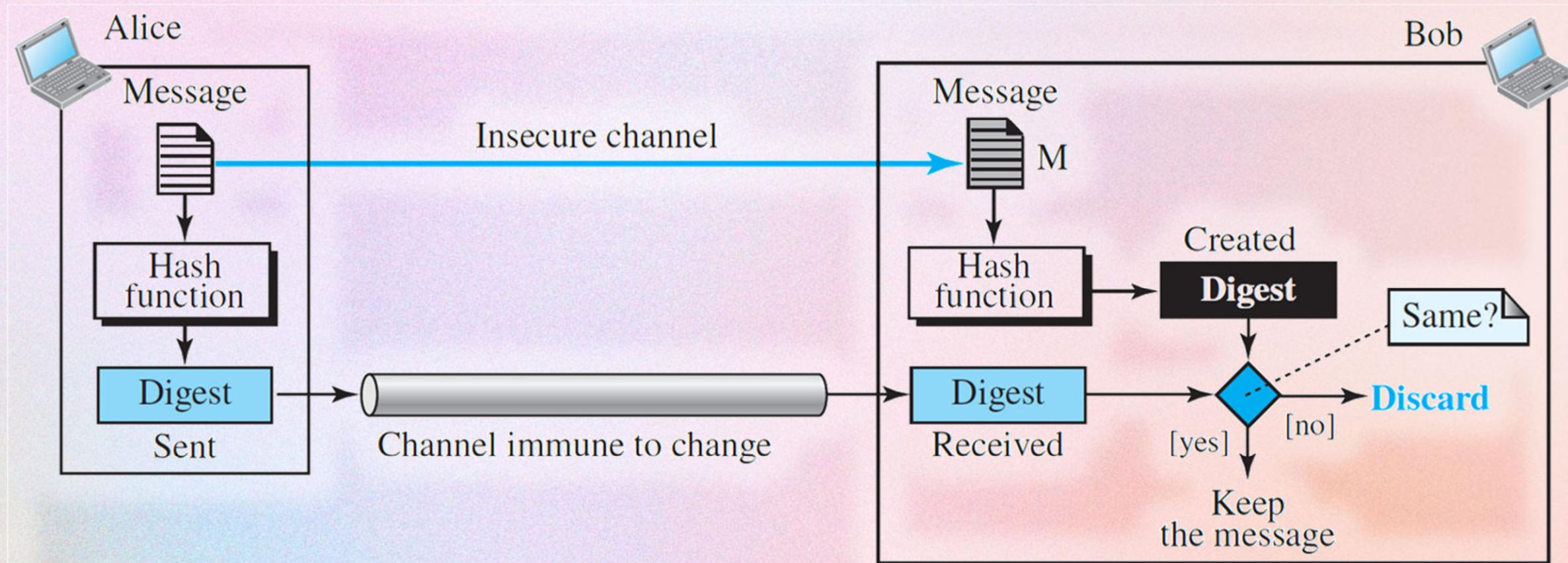


Content Curated by Pollux M. Rey

CRYPTOGRAPHIC HASH FUNCTIONS



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

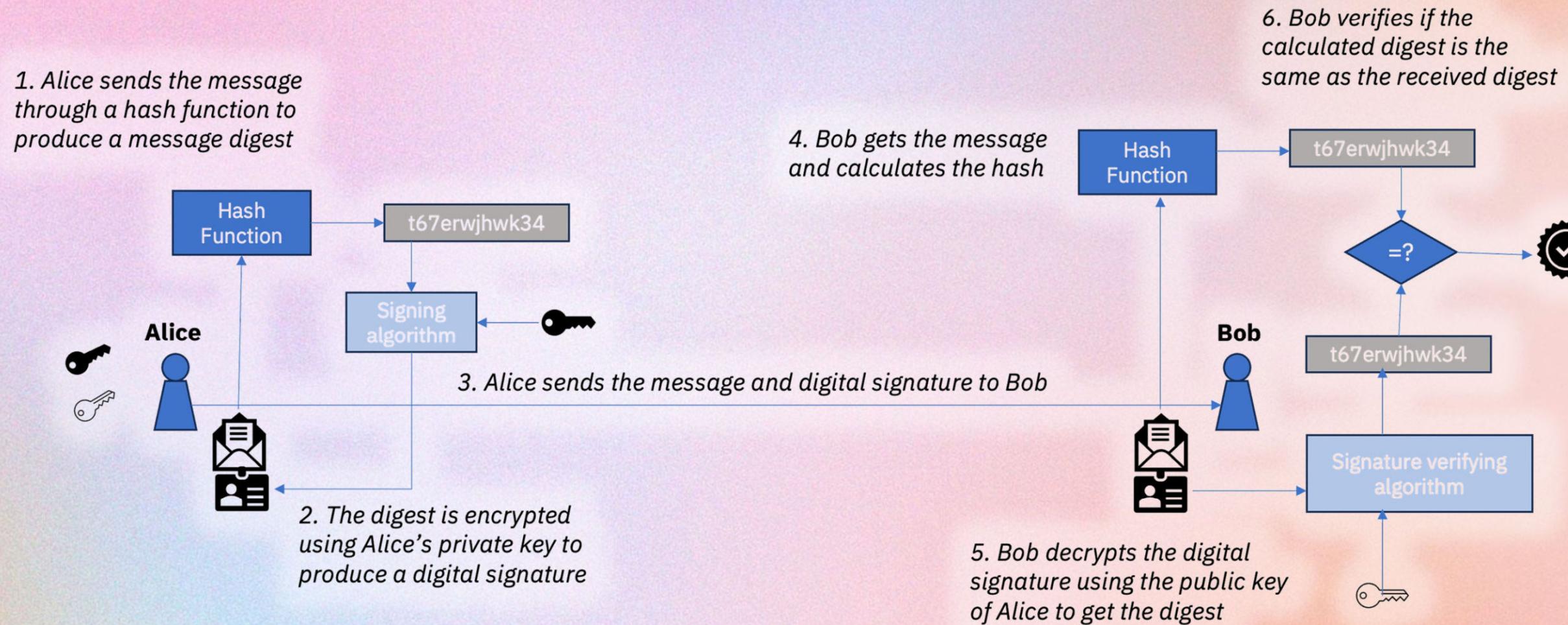


COMMONLY USED CHFs



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...

O1

**WHAT IS
A DIGITAL
SIGNATURE?**

O2

**PERSONAL VS.
DIGITAL
SIGNATURE**

O3

PROCESS

O4

**CREATING
A DIGITAL
SIGNATURE**

FOR THIS UNIT...

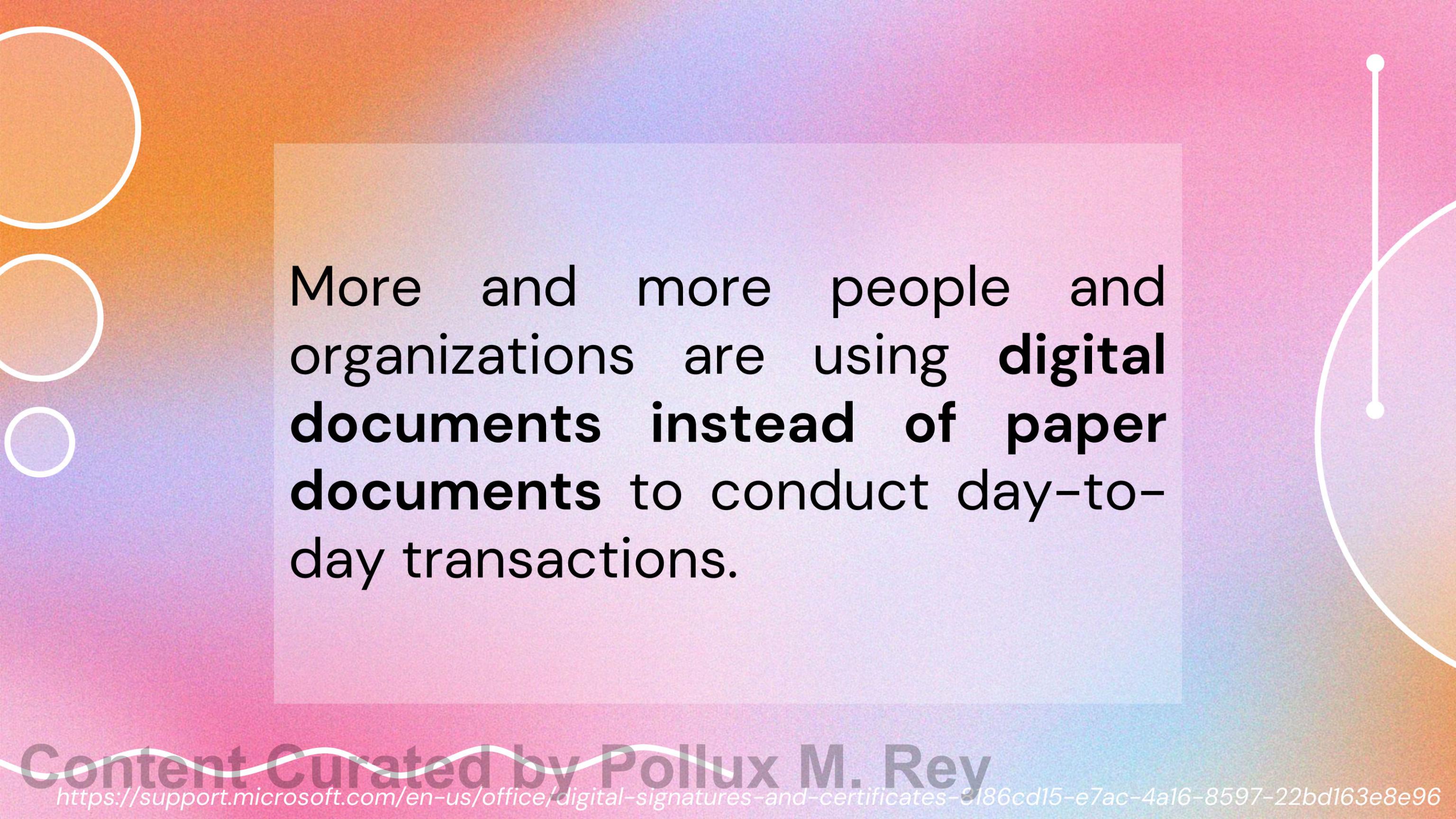
05

**DIGITAL
SIGNATURE
ASSURANCES**

Content Curated by Pollux M. Rey

01

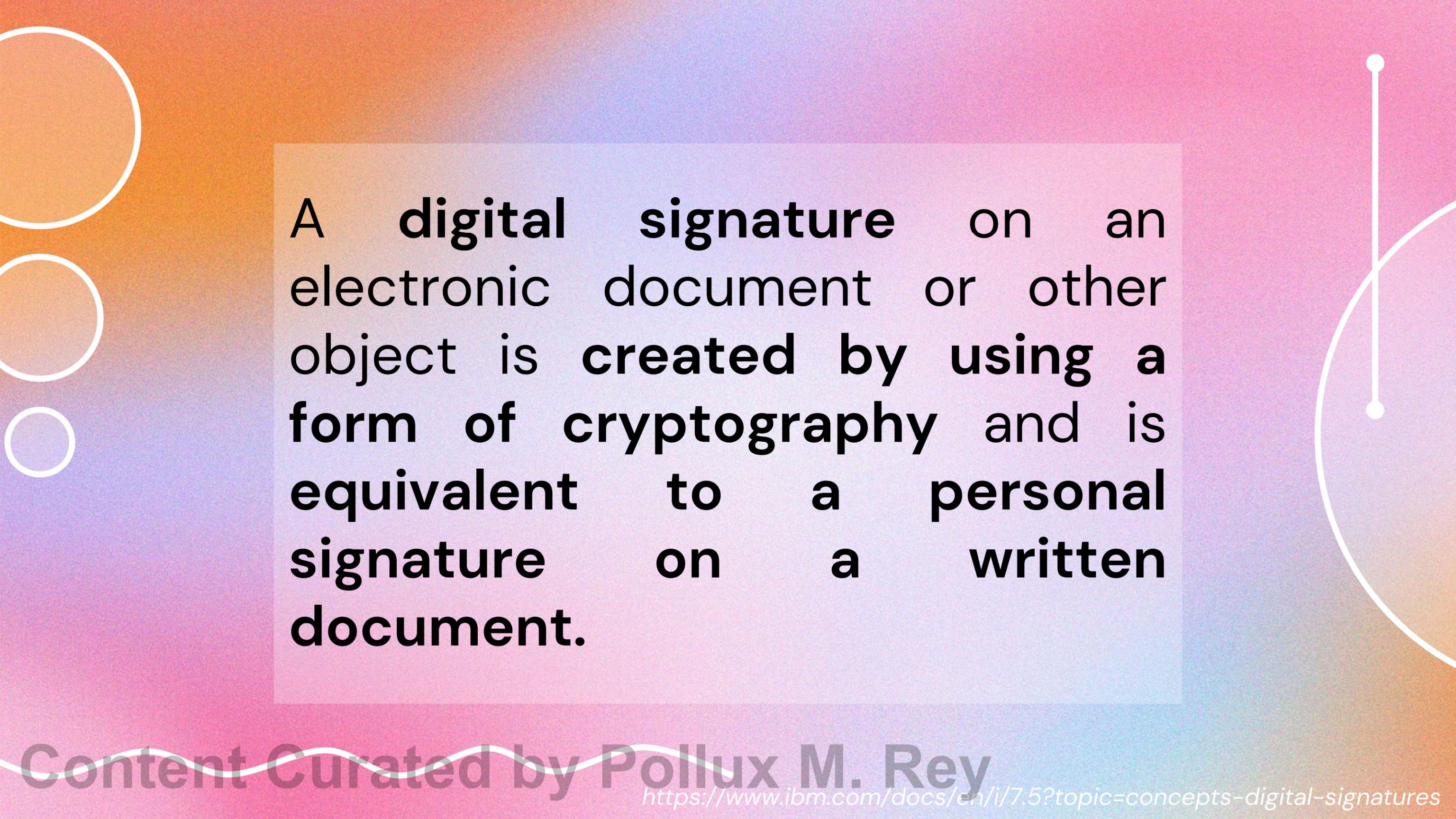
WHAT IS A DIGITAL SIGNATURE?



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



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



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.

O2

PERSONAL VS. DIGITAL SIGNATURE

Content Curated by Pollux M. Rey

CONVENTIONAL VS. DIGITAL SIGNATURES



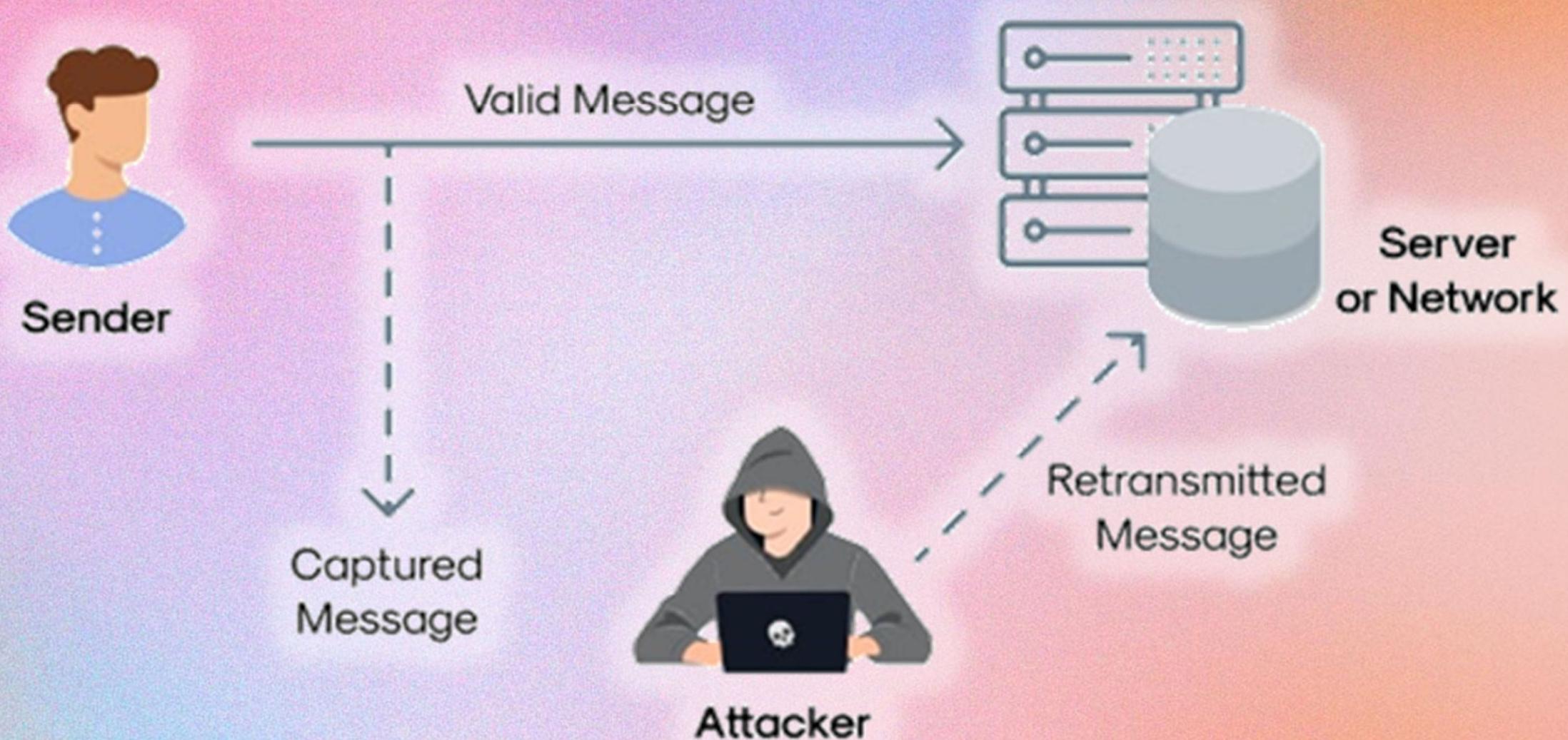
Characteristics	Conventional Signature	Digital Signature
Inclusion	Physically applied to the document itself	Added as a separate data
Verification Method	Checks the document's signature against a stored sample	Needs to apply a verification technique to the message and the signature
Relationship	One-to-many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

CONVENTIONAL VS. DIGITAL SIGNATURES



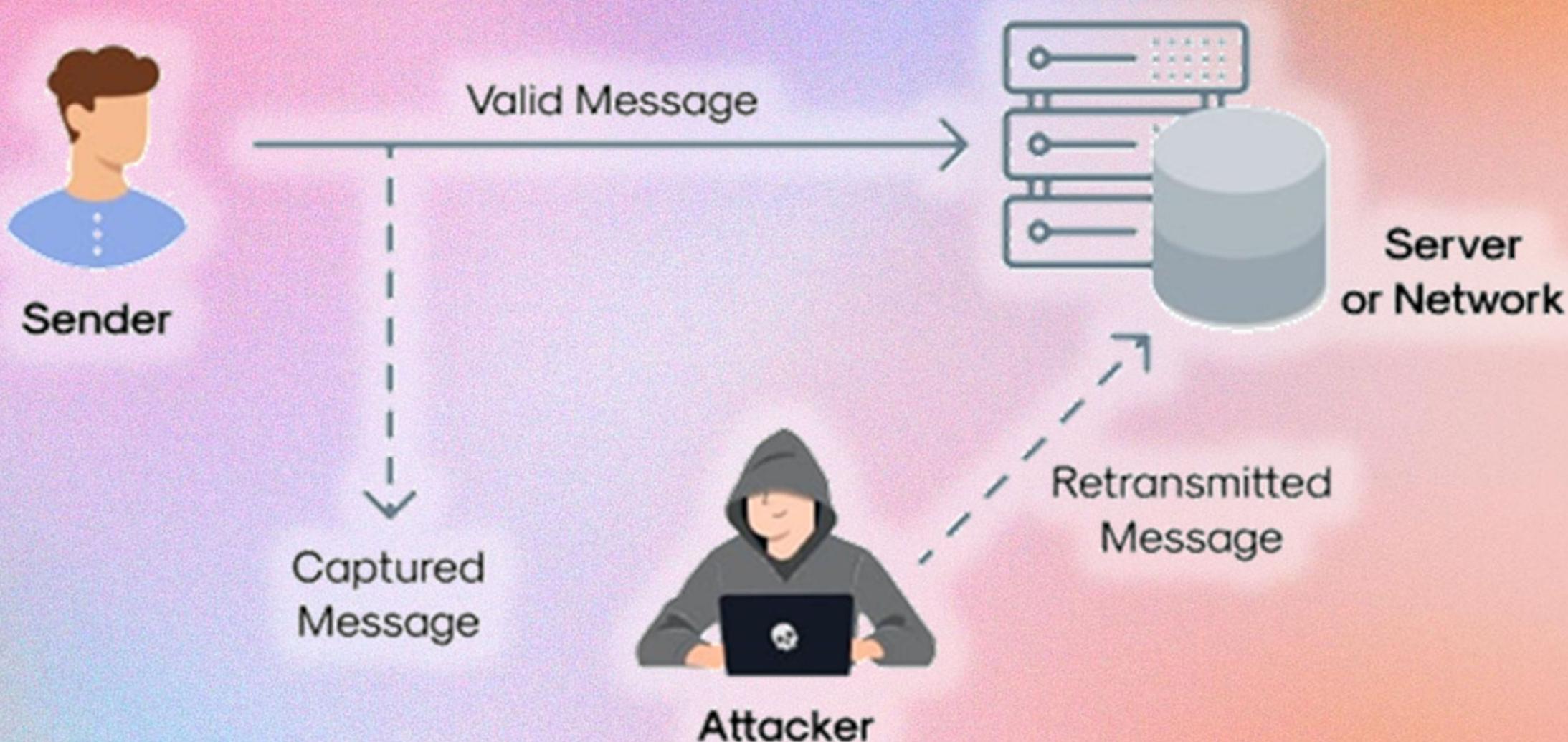
Characteristics	Conventional Signature	Digital Signature
Inclusion	Physically applied to the document itself	Added as a separate data
Verification Method	Checks the document's signature against a stored sample	Needs to apply a verification technique to the message and the signature
Relationship	One-to-many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

DUPPLICITY OF A DIGITAL SIGNATURE



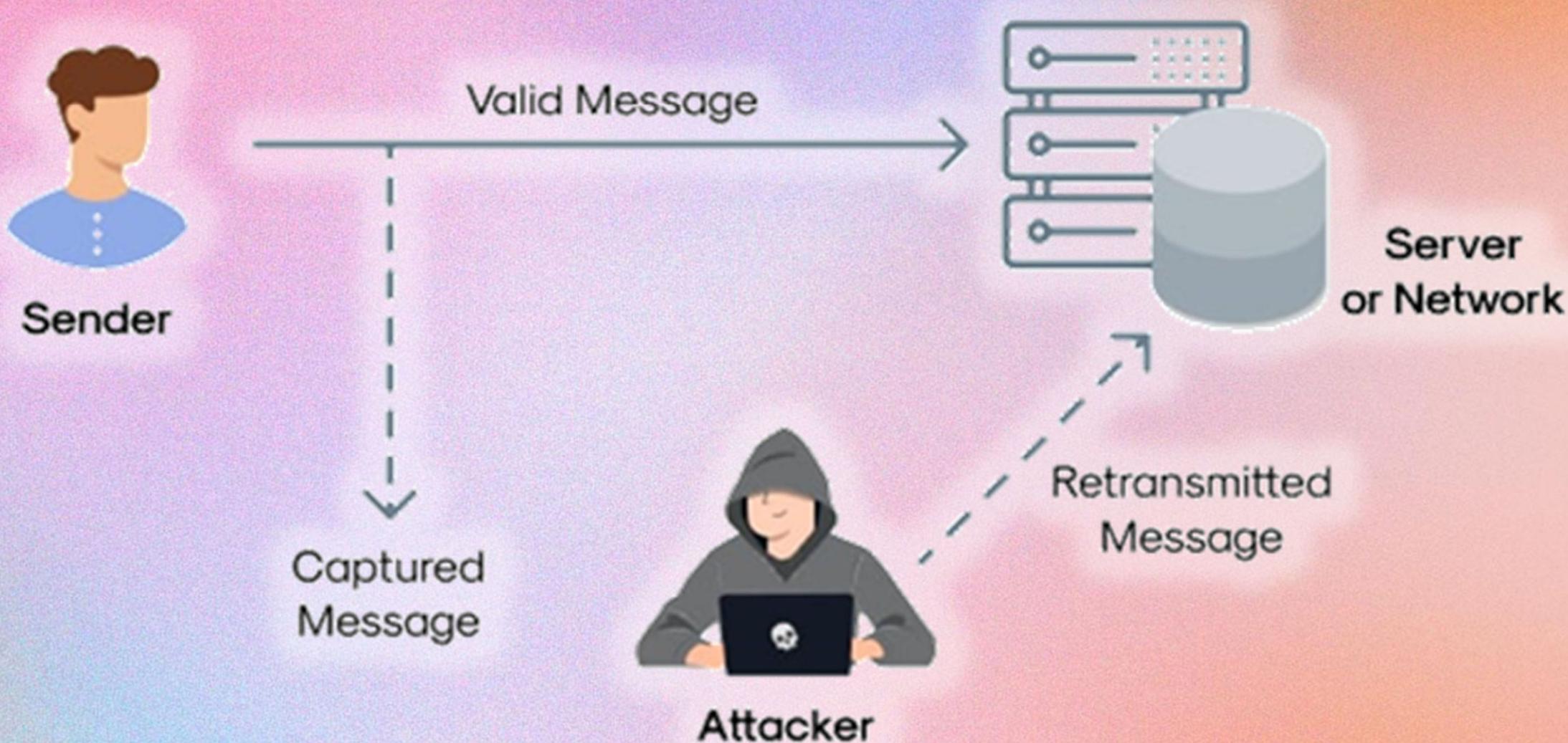
Bob (sender) sends a withdrawal request to the server.

DUPPLICITY OF A DIGITAL SIGNATURE



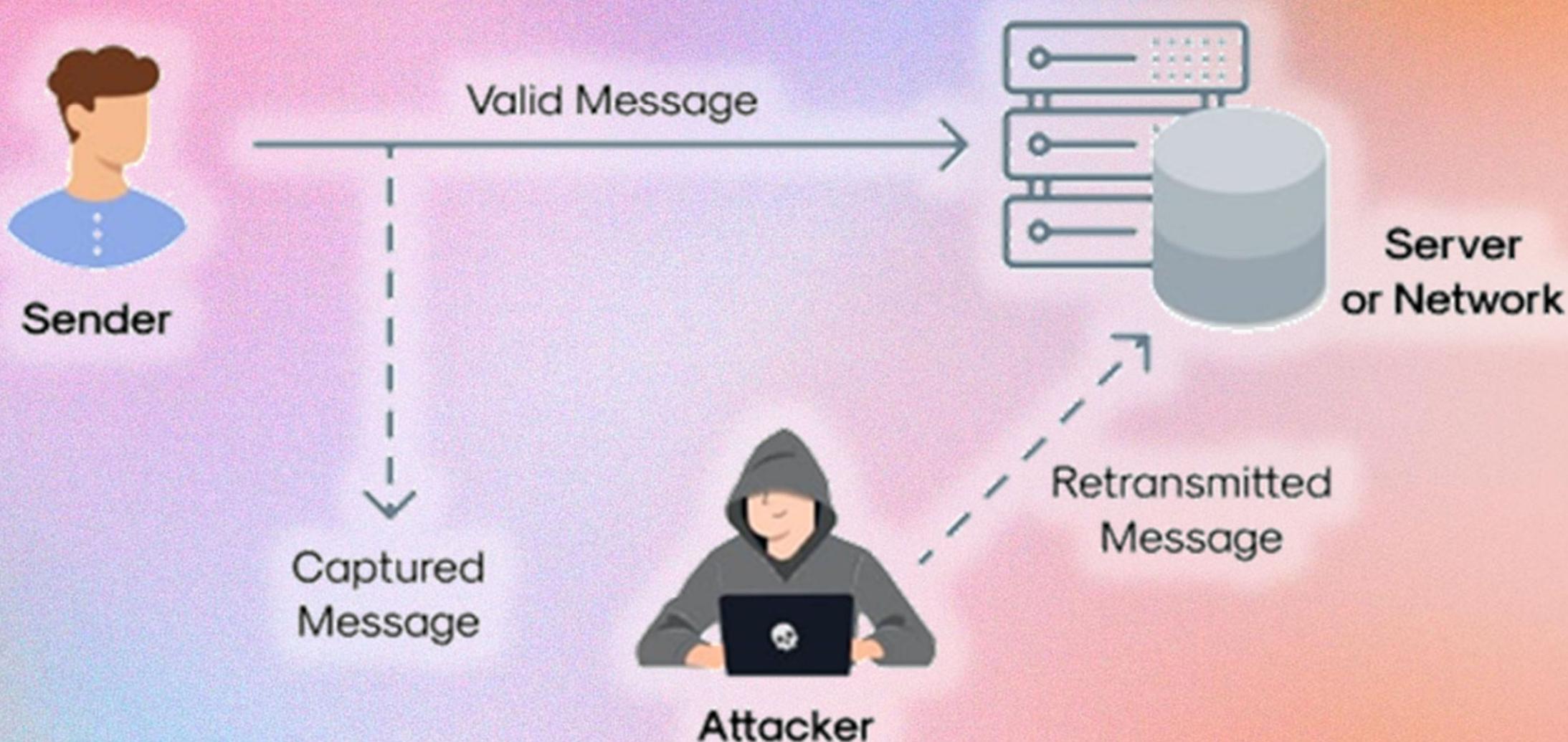
Eve (attacker) intercepts and later replays Bob's message.

DUPPLICITY OF A DIGITAL SIGNATURE



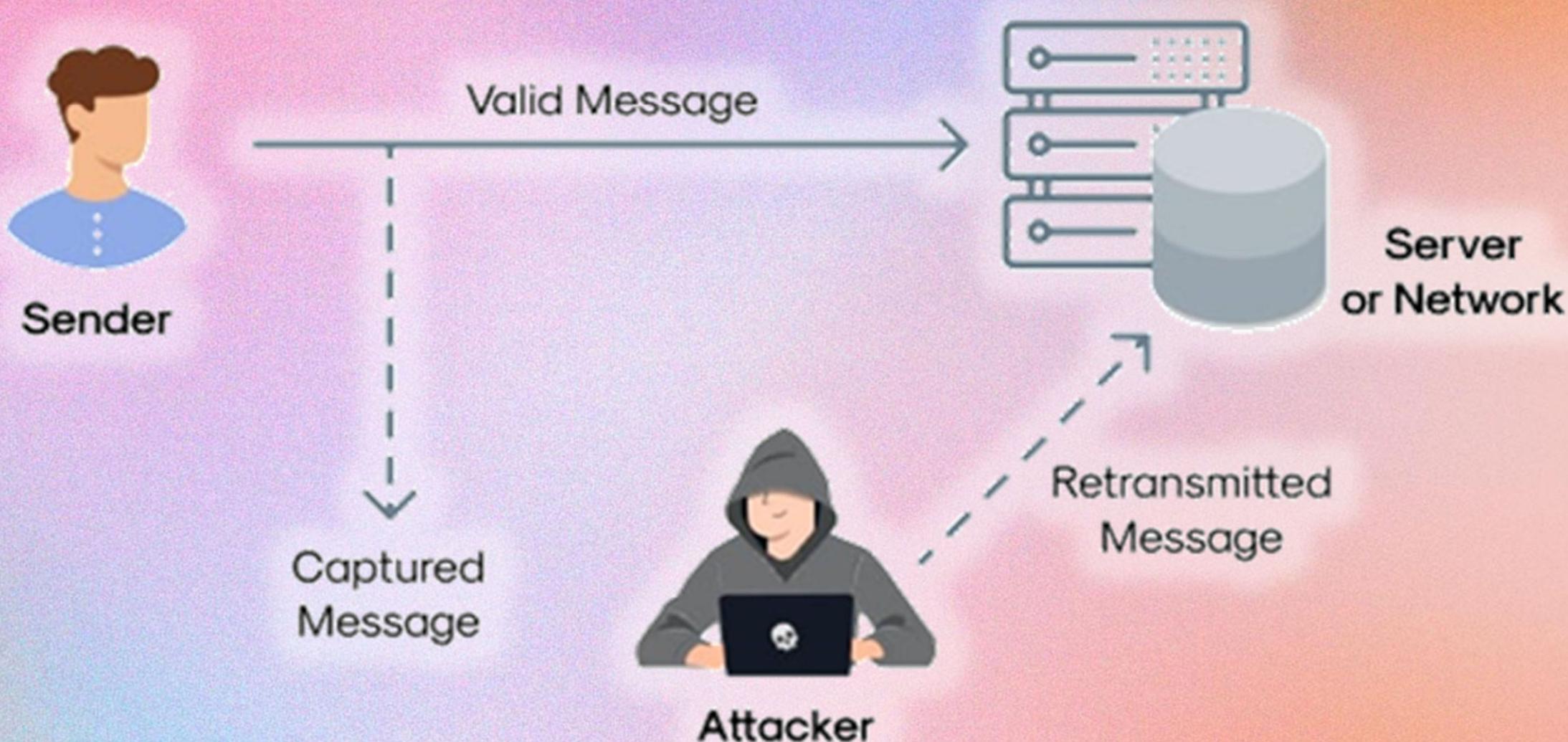
Without a timestamp, the server might process the replayed message as a new request.

DUPPLICITY OF A DIGITAL SIGNATURE



A timestamp helps the server detect
and ignore duplicate requests.

REPLAY ATTACK



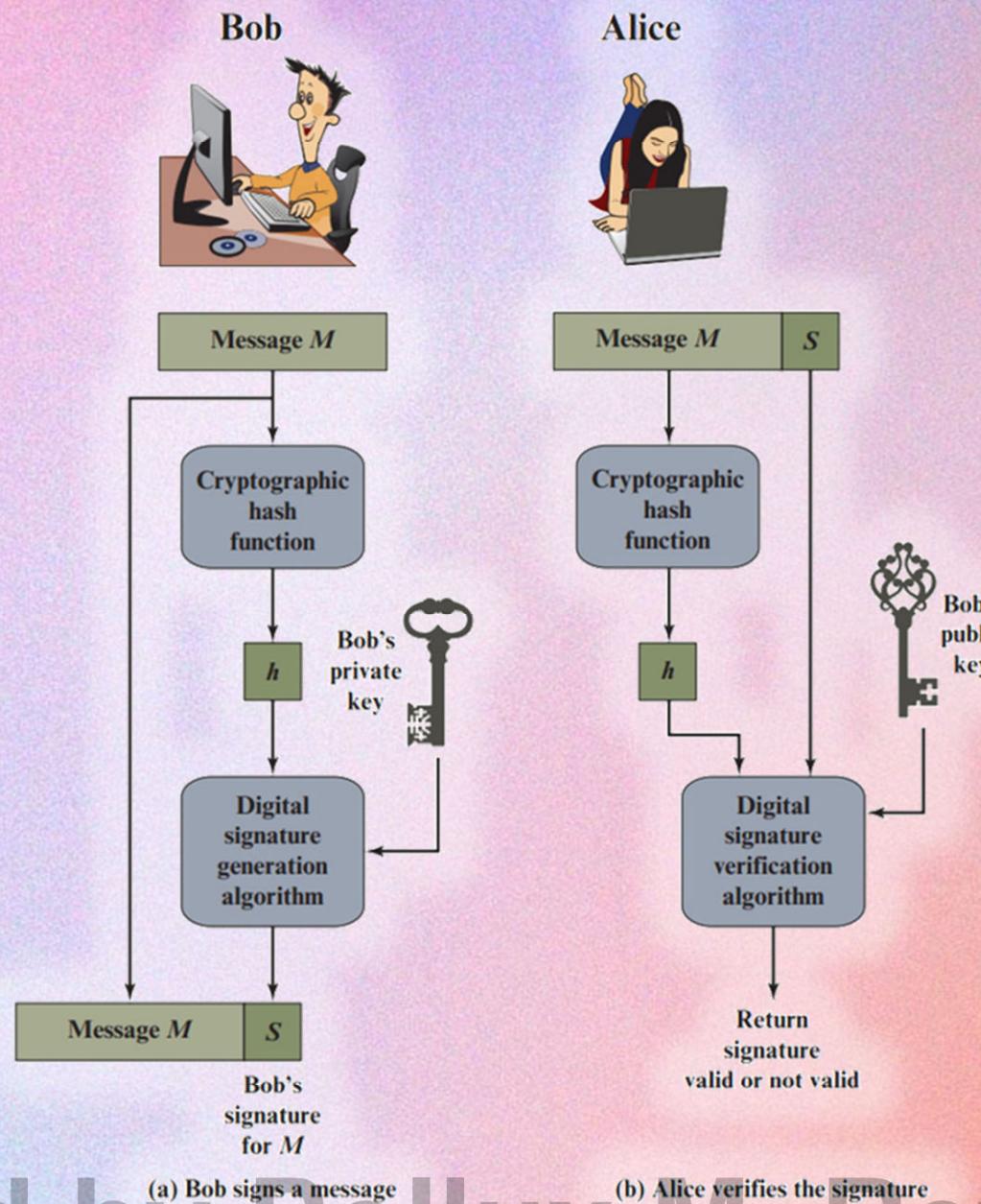
A timestamp helps the server detect
and ignore duplicate requests.

03

PROCESS OF A DIGITAL SIGNATURE

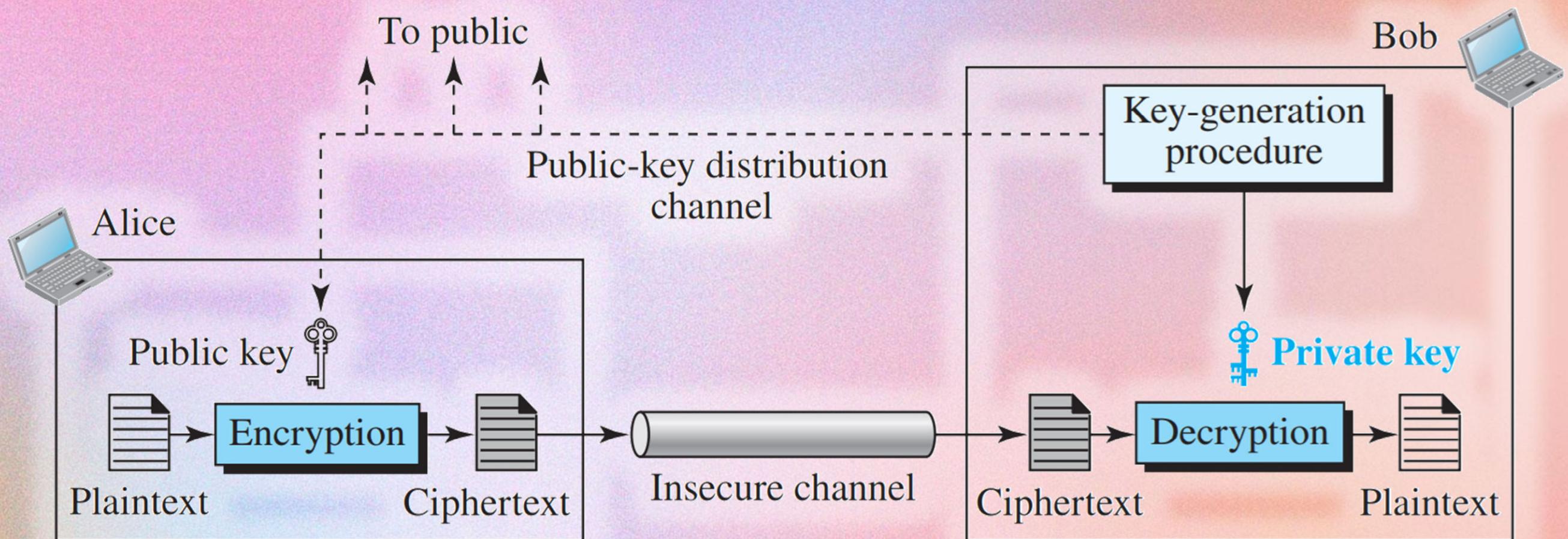
Content Curated by Pollux M. Rey

PROCESS OF A DIGITAL SIGNATURE



ASYMMETRIC-KEY CIPHER

X





RSA

Digital Signature Algorithm (DSA)

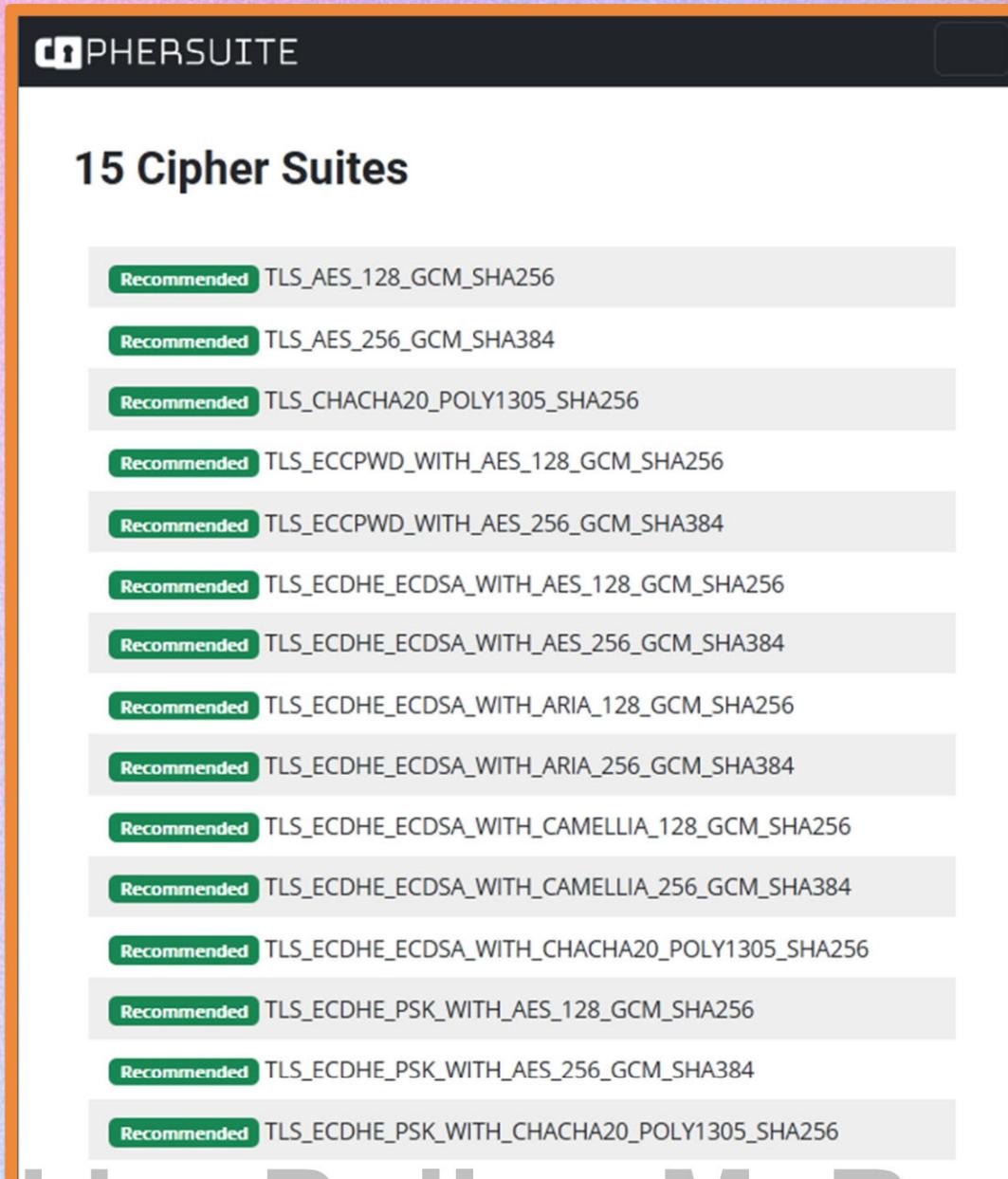
Elliptic Curve

Digital Signature Algorithm (ECDSA)

Content Curated by Pollux M. Rey

Cryptography and Network Security, Stallings

SOME DIGITAL SIGNATURE ALGORITHMS



The screenshot shows a list of 15 recommended cipher suites from the Phersuite interface. Each suite is listed in a separate row, with its status as 'Recommended' indicated in a green box. The suites are:

- Recommended TLS_AES_128_GCM_SHA256
- Recommended TLS_AES_256_GCM_SHA384
- Recommended TLS_CHACHA20_POLY1305_SHA256
- Recommended TLS_ECCPWD_WITH_AES_128_GCM_SHA256
- Recommended TLS_ECCPWD_WITH_AES_256_GCM_SHA384
- Recommended TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- Recommended TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Recommended TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
- Recommended TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
- Recommended TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- Recommended TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- Recommended TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- Recommended TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- Recommended TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384
- Recommended TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256

Content Curated by Pollux M. Rev

Data Communications And Networking, Behrouz A Forouzan

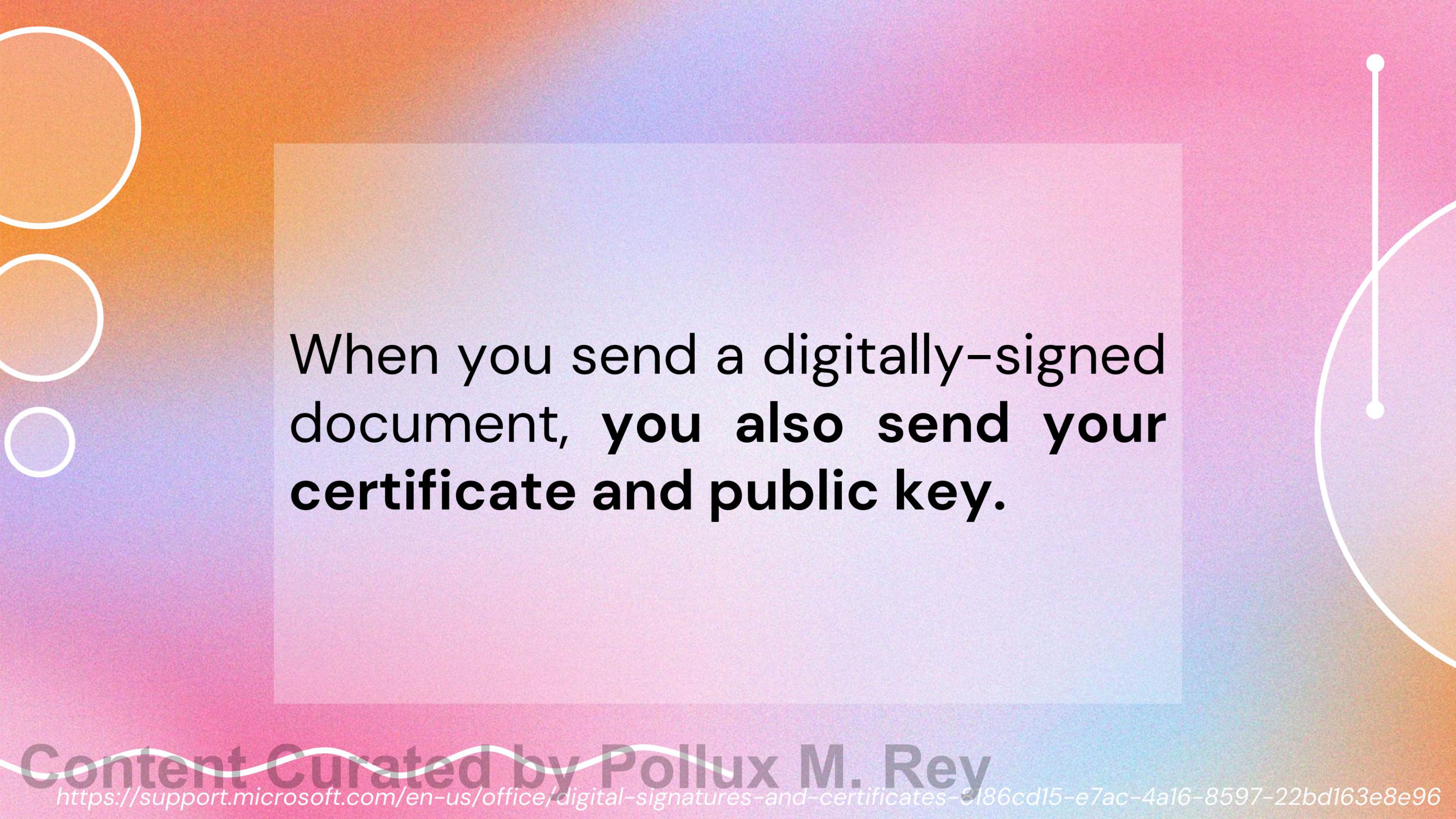
04

CREATING A DIGITAL SIGNATURE

Content Curated by Pollux M. Rey



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



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



Certificates are issued by a
certification authority (CA).

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

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



**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](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



For more info visit :
<https://dict.gov.ph/pnppki/>
E-mail: LC3.SUPPORT.PNPKI@DICT.GOV.PH
FB page: facebook.com/dictlc3/

Content Curated by Pollux M. Rey

<https://dict.gov.ph/pnppki>

PNPKI Online Registration System

Thank you for your interest in availing PNPKI individual digital certificates!

For **bulk application**, please coordinate with the PNPKI team in your respective area, email addresses can be found on this link: [\(PNPKI Contact Information\)](#).

For **NEW individual application**, please read the following guidelines before proceeding to the Registration Portal.

Applications with incomplete information and/or requirements will not be processed.

Step 0: Preparing PNPKI Requirements



Please prepare the following requirements which are required to be uploaded to the Registration portal (file format must be **LastName FirstName Document Type**. file size must be less than 5MB and accepted file types are .JPG, .JPEG, .PDF, .DOC, .DOCX):

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).

Signed and all signatures are valid.

Republic of the Philippines
MARINDUQUE STATE UNIVERSITY
COLLEGE OF INFORMATION AND COMPUTING SCIENCES
Panfilo M. Mangura Sr. Rd., Tanza, Boac, Marinduque
CICS Tel. No.: (042) 332-2853 CICS E-mail Address: cics@mscmarinduque.edu.ph
Website: www.mscmarinduque.edu.ph

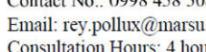
Courses Offered:
Bachelor of Science in Information Technology
BS in Information Systems
BS in Management Systems
AACCUP Accredited Level 3

Santa Cruz Campus:
BS in Information Systems
(AACCUP, Inc. Re-Accredited Level 2)

Bachelor of Science in Information Technology
(Accreditation Level III) by the Accrediting Agency for Chartered Colleges & Universities in the Philippines (AACCUP), Inc.


POLLUX M. REY
Faculty, CICS
Contact No.: 0998 458 5080
Email: rey.pollux@marsu.edu.ph
Consultation Hours: 4 hours

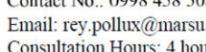
Pollux M. Rey Digitally signed by Pollux M. Rey Date: 2025.03.24 09:14:04 +08'00'



At least one signature is invalid.

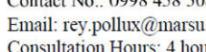
Republic of the Philippines
MARINDUQUE STATE UNIVERSITY
COLLEGE OF INFORMATION AND COMPUTING SCIENCES
Panfilo M. Mangura Sr. Rd., Tanza, Boac, Marinduque
CICS Tel. No.: (042) 332-2853 CICS E-mail Address: cics@mscmarinduque.edu.ph
Website: www.mscmarinduque.edu.ph

Bachelor of Science in Information Technology
(Accreditation Level III) by the Accrediting Agency for Chartered Colleges & Universities in the Philippines (AACCUP), Inc.


POLLUX M. REY
Faculty, CICS
Contact No.: 0998 458 5080
Email: rey.pollux@marsu.edu.ph
Consultation Hours: 4 hours

Pollux M. Rey Digitally signed by Pollux M. Rey Date: 2025.03.24 09:14:04 +08'00'

Tampere



Signatures

- Rev. 1: Signed by Pollux M. Rey <rey.pollux@marsu.edu.ph>
 - Signature is invalid:
 - Document has been altered or corrupted since it was signed
 - Signed by the current user
 - Signing time is from the clock on the signer's computer
 - Signature is LTV enabled

Signature Details

- Certificate Details...
 - Last Checked: 2025.03.24 09:19:36 +08'00'
 - Field: Signature2 on page 11
 - Click to view this version

Annotations Created

- FreeText annot on page 11
- Document Locked by Signature2

Content Curated by Pollux M. Rey



A graphic design featuring a pink-to-white gradient background with white wavy lines at the top and bottom. In the center-left, a yellow-to-orange gradient rectangular area contains the text "THANK YOU!". To the right, there are three overlapping white-outlined circles of increasing size. A thin white horizontal line with small circular caps extends from the left edge of the yellow area to the right edge of the circles.

**THANK
YOU!**

Content Curated by Pollux M. Rey