INTRODUCTION TO CRYPTOGRAPHY

FOR TODAY...

01 DEFINITION OF CRYPTOGRAPHY

02 HISTORY

03 ROLE

04 KEY CONCEPTS

05 FUNDAMENTAL PRINCIPLES

06 CATEGORIES OF CRYPTOGRAPHIC SYSTEMS

01

WHAT IS CRYPTOGRAPHY?

Content Curated by Pollux M. Rey

CRYPTOGRAPHY

Greek words

"kryptos" + "graphein"

hidden *to write*

Content Curated by Pollux M. Rey

https://www.ibm.com/think/topics/cryptography-history

CRYPTOGRAPHY

The practice of **encrypting transmitted information** so that **it can only be interpreted by the intended recipient.**

Content Curated by Pollux M. Rey

https://www.ibm.com/think/topics/cryptography-history

02

HISTORY OF CRYPTOGRAPHY

Content Curated by Pollux M. Rey

ANCIENT CRYPTOGRAPHY

1900 BC

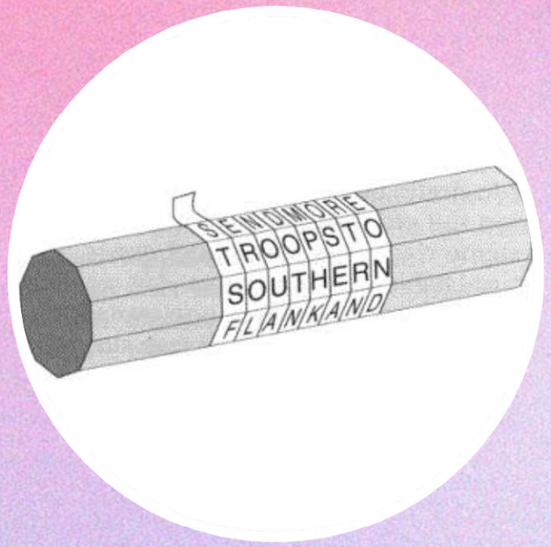
Non-standard hieroglyphs on an Old Kingdom Egyptian tomb wall

1500 BC

Enciphered writing on **Mesopotamian clay tablets**

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

ANCIENT CRYPTOGRAPHY



650 BC

Ancient Spartans used a **scytale** to encrypt military messages

100-44 BC

Caesar Cipher was used to secure communications within the Roman army

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

MEDIEVAL CRYPTOGRAPHY

800

Al-Kindi invented **frequency analysis** for cipher breaking

1500

Vigenère Cipher is the landmark polyalphabetic cipher of the 16th century

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

MODERN CRYPTOGRAPHY

1917

Edward Hebern created the **first cryptography rotor machine**

1918

Enigma Machine was widely used by Germans before and during WWII

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

MODERN CRYPTOGRAPHY

1975
IBM developed the **Data Encryption Standard (DES)**

1976
The **Diffie-Hellman key exchange method** was introduced

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

MODERN CRYPTOGRAPHY

1977
RSA public key cryptosystem was introduced

1976
DES was replaced by the **Advanced Encryption Standard (AES)**

https://www.ibm.com/think/topics/cryptography-history
https://www.redhat.com/en/blog/brief-history-cryptography

03

ROLES OF CRYPTOGRAPHY IN CYBERSECURITY

Content Curated by Pollux M. Rey

```
{
    "strength": "N/A",
    "weakness": "Hindi marunong makaunawa sa sitwasyon ng istudyante nya!!!",
    "evaluation":{
        "1": [1,1,1,1,1],
        "2": [1,1,1,1,1],
        "3": [1,1,1,1,1],
        "4": [1,1,2,1,1]},
    "comments": null,
    "categoryId": null,
    "studentId": 3549,
    "instructorId": 18382,
    "sectionId": 46604,
    "subjectId": 16060,
    "semesterId": 296,
    "schoolYearId": 1055,
    "stars": null,
    "createdById": null,
    "signatureUpload": null,
    "modifiedById": null,
    "status": true,
    "_id": 1204810,
    "comment": null,
    "createdDate": "2024-12-09T07:05:39.338Z",
    "modifiedDate": "2024-12-09T07:05:39.338Z"
}
```

```
{
    "avatar": null,
    "signature": null,
    "studentNumber": "22B****",
    "firstName": "**** ******",
    "middleName": "******",
    "lastName": "******",
    "extension": null,
    "gender": null,
    "civilStatus": null,
    "birthDate": null,
    "birthPlace": null,
    "email": "**************@mscmarinduque.edu.ph",
    "contactNumber": null,
    "nationality": null,
    "religion": null,
    "address": null,
    "guardianId": null,
    "isActive": true,
    "_id": 3549,
    "campusId": 2,
    "collegeId": 2019,
    "courseId": 4999,
    "admittedYearId": 940,
    "admittedSemId": 296,
    "createdById": 12856,
    "modifiedById": 12856,
    "userId": 35508,
    "createdAt": "2024-07-10T16:52:19.367Z",
    "updatedAt": "2024-09-17T08:55:01.890Z"
}
```

```
{
    "_id": 30344,
    "email": "*****.***@marsu.edu.ph",
    "password": "$2b$12$A0Ppe4/vifZ1CVjetVHXG.0ztMcbbTGgLTt21jDtIyxRKldYw/./m",
    "temporaryPassword": "**********",
    "firstName": "***",
    "middleName": "*******",
    "lastName": "*****",
    "passwordResetToken": null,
    "avatar": null,
    "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjMwMzQ0LCJkYXRlIjoiMjAyNC0xMi0wOVQwMTo0NjowMy44MDda
IiwiaWF0IjoxNzMzNzA4NzYzLCJleHAiOjE3MzQzMTM1NjN9.m18KI4PmQXFLFR7C5TNOl6q2mY21A9w0GgswCAup1N8",
    "lastLogin": "2024-12-09T01:46:03.807Z",
    "contactNo": "**********",
    "invalidAttempts": 0,
    "iamAdmin": true,
    "adminScopes": [
        "IAM",
        "CAMPUS",
        "CHATBOT",
        "SUPPORT",
        "FRS",
        "DATA",
        "REPORTS"
    ],
    "loggedIn": true,
    "active": true,
    "createdById": 12856,
    "modifiedById": 12856,
    "enable2FA": false,
    "secretkey2FA": "false",
    "updatedAt": "2024-12-09T01:46:03.807Z",
    "createdAt": "2024-06-08T07:24:34.845Z"
}
```

OWASP PROJECTS CHAPTERS EVENTS ABOUT Store Donate Join

OWASP Top Ten

Main | Translation Efforts | Sponsors | Data 2025

Important note:

OWASP Top Ten 2025

Current project status as of September 2024:

- We are planning to announce the release of the **OWASP Top 10:2025** in the first half of 2025.
- **Data Collection (Now - December 2024)**: Please donate your application penetration testing statistics.

Stay Tuned!

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

> Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Watch 325 Star 1,138

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Information

- OWASP Top 10:2021
- Making of OWASP Top 10
- OWASP Top 10:2021 - 20th Anniversary Presentation (PPTX)

Flagship Project
Documentation
Builder
Defender

- Previous Version (2017)

Downloads or Social Links

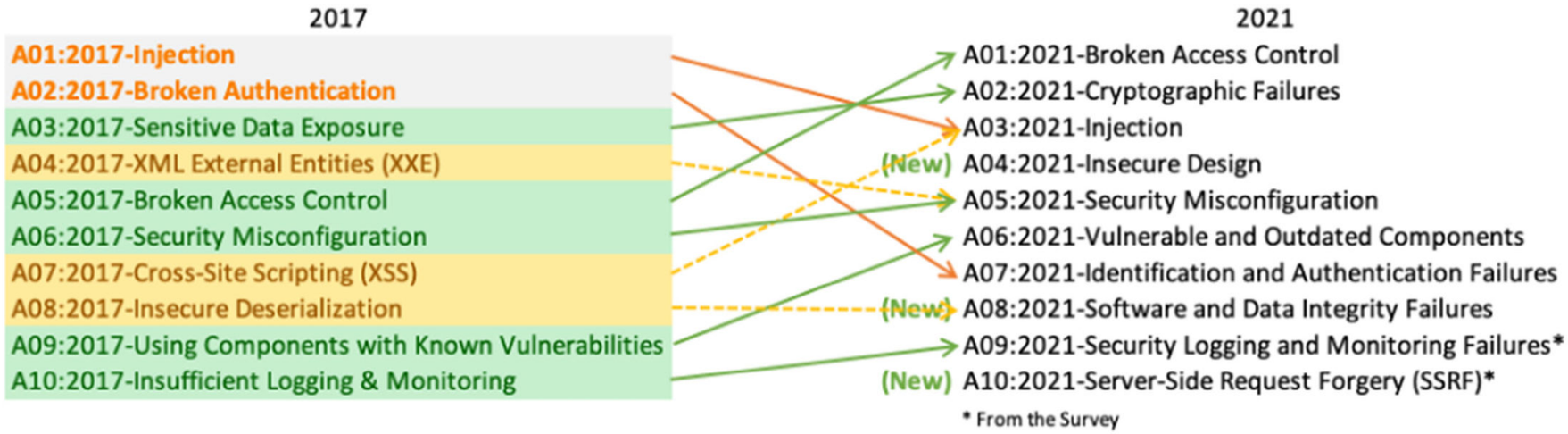
- OWASP Top 10 2017
- Other languages → tab 'Translation Efforts'

Social

https://owasp.org/www-project-top-ten

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.

https://owasp.org/www-project-top-ten

A02 Cryptographic Failures

OWASP/Top10
☆ 4.4k ⑂ 846

Description

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS). For all such data:

- Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, FTP also using TLS upgrades like STARTTLS. External internet traffic is hazardous. Verify all internal traffic, e.g., between load balancers, web servers, or back-end systems.
- Are any old or weak cryptographic algorithms or protocols used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing? Are crypto keys checked into source code repositories?
- Is encryption not enforced, e.g., are any HTTP headers (browser) security directives or headers missing?
- Is the received server certificate and the trust chain properly validated?
- Are initialization vectors ignored, reused, or not generated sufficiently secure for the cryptographic mode of operation? Is an insecure mode of operation such as ECB in use? Is

https://owasp.org/Top10/A02_2021-Cryptographic_Failures

How to Prevent

Do the following, at a minimum, and consult the references:

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
- Encrypt all data in transit with secure protocols such as TLS with forward secrecy (FS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Disable caching for response that contain sensitive data.
- Apply required security controls as per the data classification.
- Do not use legacy protocols such as FTP and SMTP for transporting sensitive data.
- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2.

https://owasp.org/Top10/A02_2021-Cryptographic_Failures

04

KEY CONCEPTS

Content Curated by Pollux M. Rey

GENERAL IDEA OF A SYMMETRIC-KEY CIPHER

CIPHER: *encryption and decryption algorithms*

GENERAL IDEA OF A SYMMETRIC-KEY CIPHER

PLAINTEXT: *original message*

GENERAL IDEA OF A SYMMETRIC-KEY CIPHER

CIPHERTEXT: *coded message*

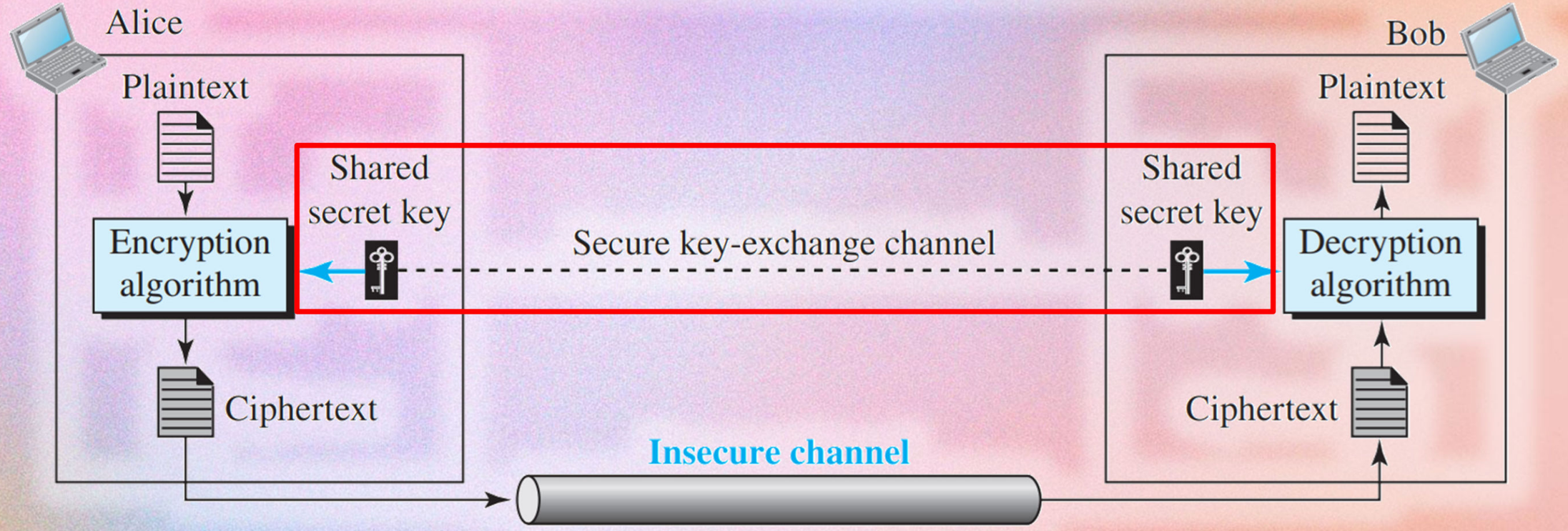
GENERAL IDEA OF A SYMMETRIC-KEY CIPHER

ENCRYPTION: *process of converting from plaintext to ciphertext*

GENERAL IDEA OF A SYMMETRIC-KEY CIPHER

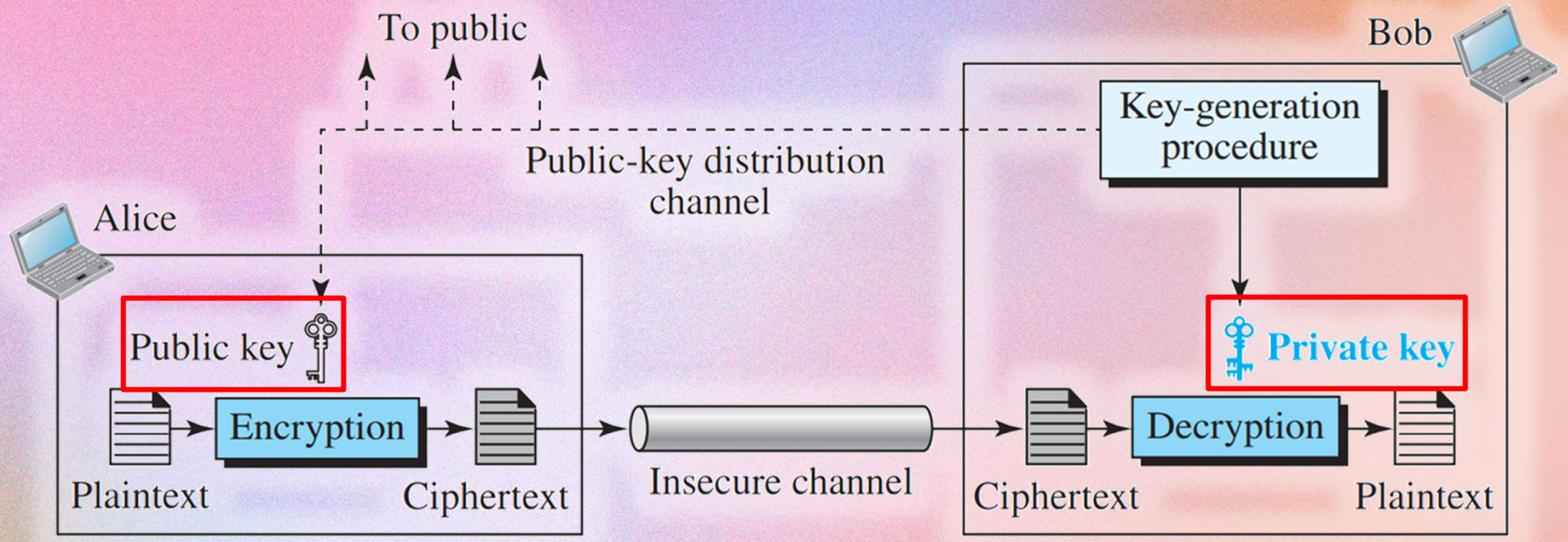
DECRYPTION: *process of converting from ciphertext to plaintext*

GENERAL IDEA OF A SYMMETRIC-KEY CIPHER



SYMMETRIC-KEY CIPHER: *uses the same key for both encryption and decryption*

GENERAL IDEA OF AN ASYMMETRIC-KEY CIPHER



ASYMMETRIC-KEY CIPHER: *uses the **public key** for encryption and the **private key** for decryption*

05

HOW DOES CRYPTOGRAPHY RELATE TO INFORMATION ASSURANCE AND SECURITY?

Content Curated by Pollux M. Rey

INFORMATION SECURITY

An umbrella term that covers an organization's efforts to **protect information.**

Content Curated by Pollux M. Rey

https://www.ibm.com/think/topics/information-security

INFORMATION SECURITY

It includes physical IT asset security, endpoint security, **data encryption**, network security and more.

Content Curated by Pollux M. Rey

https://www.ibm.com/think/topics/information-security

INFORMATION SECURITY

Information security practices are based on decades-old, evolving principles:

CIA Triad

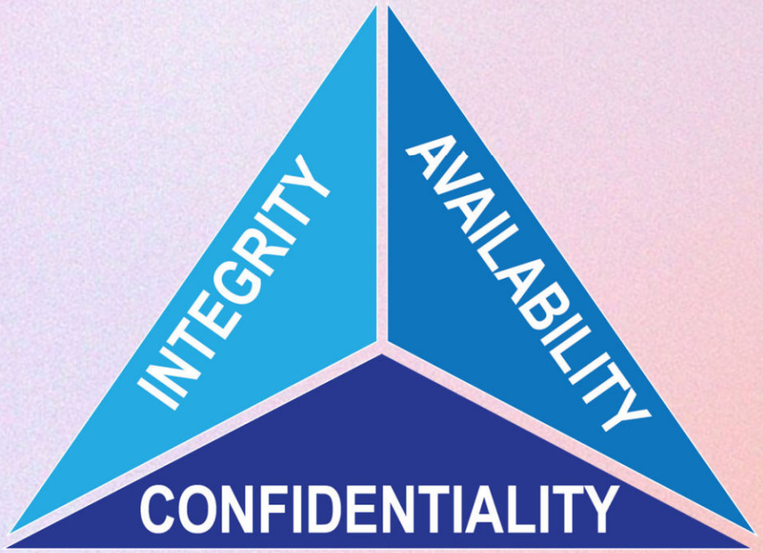
Information Assurance

Nonrepudiation

https://www.ibm.com/think/topics/information-security

CIA TRIAD

Intended to **guide organizations**
in choosing technologies, policies and practices
to protect their information systems.



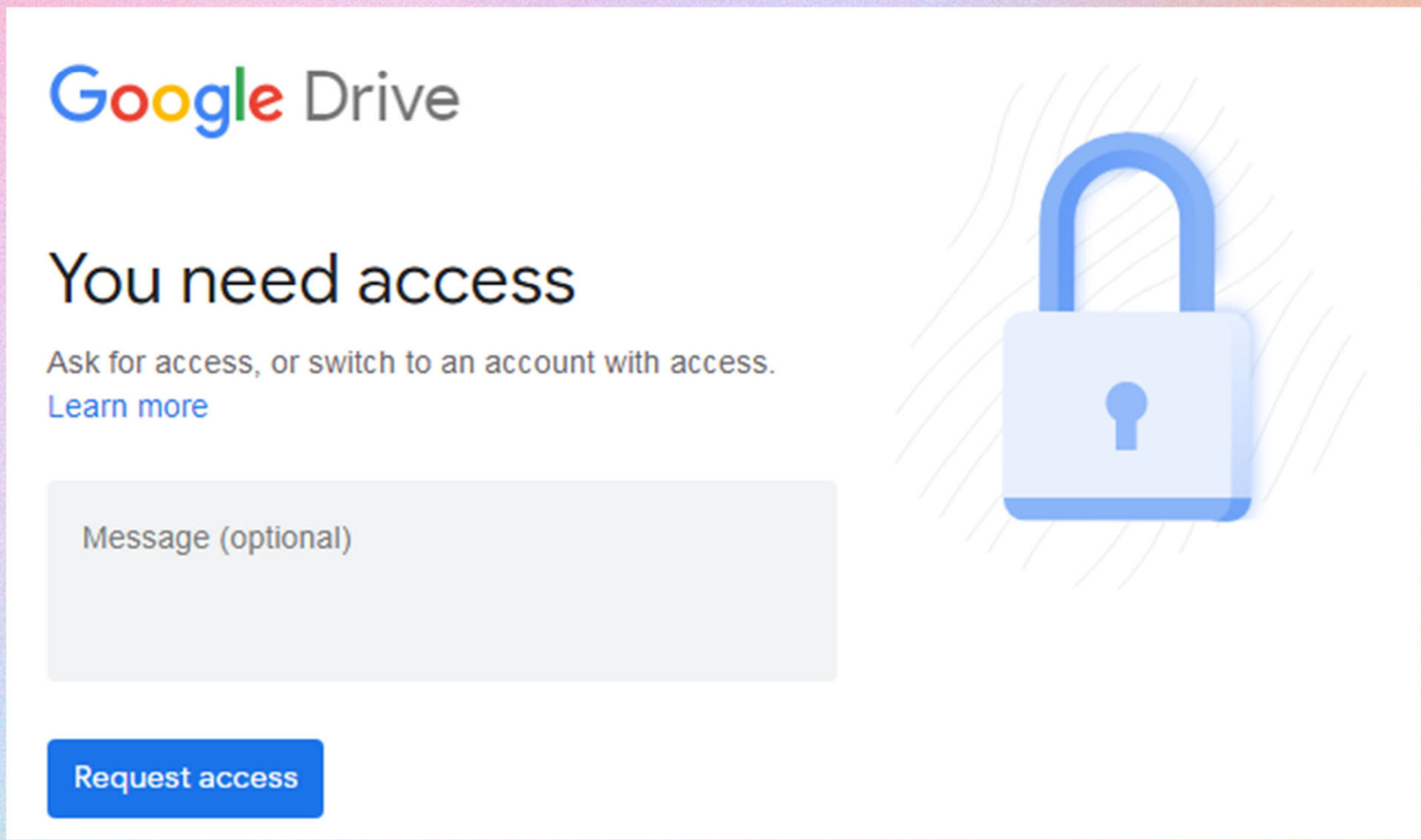
https://www.nist.gov/image/cia-triad

CIA TRIAD

Confidentiality	Parties **cannot access data they're not authorized** to access.
Integrity	All information contained within company databases is **complete and accurate.**
Availability	Users can access the information they're authorized to access **when they need it.**

https://www.ibm.com/think/topics/information-security

CONFIDENTIALITY



INTEGRITY

GMA News
October 20, 2018 ·

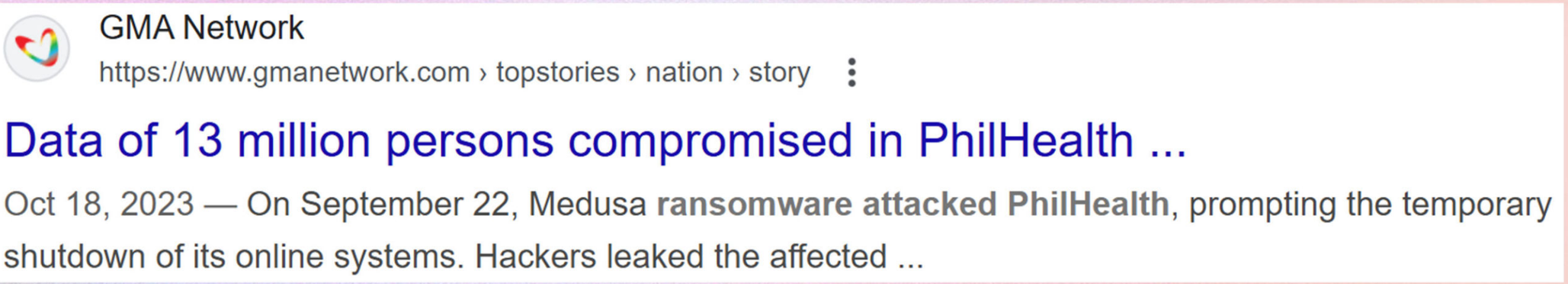
LOOK: Isang pang BPI account holder ang naging "instant millionaire" matapos magkaroon ng glitch ang BPI kagabi. Naging mahigit pitong milyong piso ang laman ng kaniyang account mula sa P27,000 na balance nito.

Kinumpirma ng BPI na nagkaroon nga ng glitch kagabi. Ayon sa opisyal ng BPI, naayos na nila ang problema kanina 4:30 ng madaling araw. | via Bernadette Reyes/GMA News

BASAHIN: http://bit.ly/2EBvs5r

See Translation

AVAILABILITY

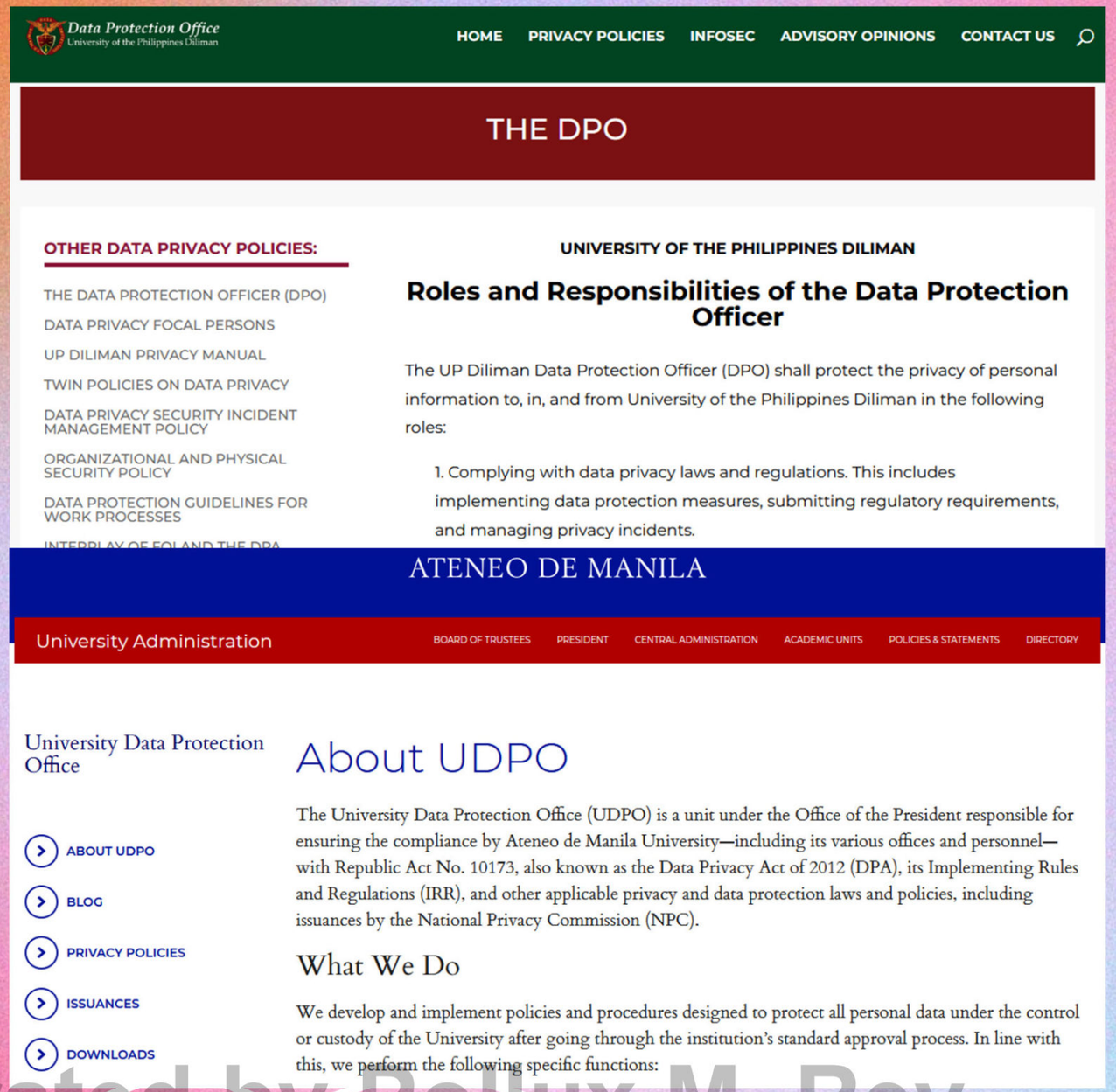


INFORMATION ASSURANCE

The practice of **managing information-related risks** and the **steps involved to protect information systems.**

Content Curated by Pollux M. Rey

https://www.itgovernanceusa.com/information/information-assurance



NONREPUDIATION

A user **cannot deny having made a transaction.**

Content Curated by Pollux M. Rey

https://www.ibm.com/think/topics/information-security

INFORMATION SECURITY VS. CRYPTOGRAPHY

Information Security		Cryptography	
Confidentiality	Parties **cannot access data they're not authorized** to access.	**Encryption Algorithms**	Performs the **transformation of data into ciphertext.**
Integrity	All information contained within company databases is **complete and accurate.**	**Hash Functions**	Transforms an input into **a string of characters of a fixed length.**
		Digital Signature	A **message digest encrypted with the message sender's private key.**

https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

INFORMATION SECURITY VS. CRYPTOGRAPHY

Information Security		Cryptography	
Nonrepudiation	A user **cannot deny having made a transaction.**	**Digital Signature**	**A message digest encrypted with the message sender's private key.**

https://www.ibm.com/think/topics/cryptography
https://www.ibm.com/think/topics/information-security
https://www.ibm.com/docs/en/cics-ts/5.6?topic=protection-digital-signatures

06

CATEGORIES OF CRYPTOGRAPHIC SYSTEMS

Content Curated by Pollux M. Rey

CLASSICAL VS. MODERN CRYPTOGRAPHY

CLASSICAL CRYPTOGRAPHY

- Treated as an **art.**
- Used primarily for **secret military communication.**
- Relied on **pencil and paper.**
- Used the **same key for both encryption and decryption.**

MODERN CRYPTOGRAPHY

- Treated as a **science.**
- Solves **confidentiality, authentication, and secure protocols.**
- **Powered by computers and complex algorithms.**
- Offers **different key options** for encryption (public key) and decryption (private key).

Cracking Codes with Python, Sweigrart
https://documents.uow.edu.au/~fuchun/book/Lecture1-PS.pdf
https://www.cse.iitd.ac.in/~siy107537/sil765/PDF/1-Provable-Security.pdf

SUBSTITUTION VS. TRANSPOSITION CIPHER

SUBSTITUTION CIPHER

- **Replaces** each letter in the plaintext with a different one.
- Examples: Caesar, Vigenère, Playfair ciphers

TRANSPOSITION CIPHER

- **Rearranges** the letters of the plaintext
- Example: Rail fence cipher

MONOALPHABETIC VS. POLYALPHABETIC

MONOALPHABETIC SUBSTITUTION CIPHER

- Substitution is **fixed** for each letter of the alphabet.
- Can be broken down using **frequency analysis.**
- Example: Caesar cipher

POLYALPHABETIC SUBSTITUTION CIPHER

- **Encoded with multiple letters**, switching between them in a systematic way.
- Example: Vigenère cipher

https://crypto.interactive-maths.com

https://pi.math.cornell.edu/~mec/2003-2004/cryptography/polyalpha/polyalpha.html

STREAM VS. BLOCK CIPHERS

STREAM CIPHER

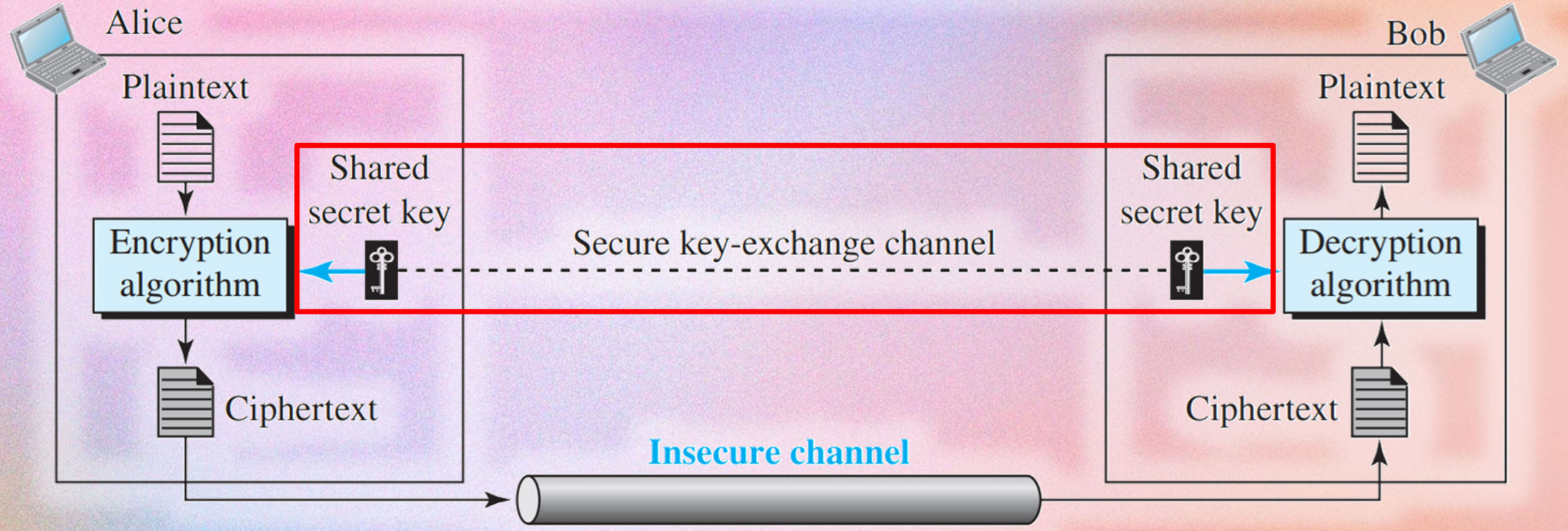
- **Converts one symbol of plaintext directly** into a symbol of ciphertext.
- Examples: Caesar, Vigenère cipher

BLOCK CIPHER

- **Encrypts a group of plaintext symbols** as one block.
- Examples: Playfair cipher, DES, AES

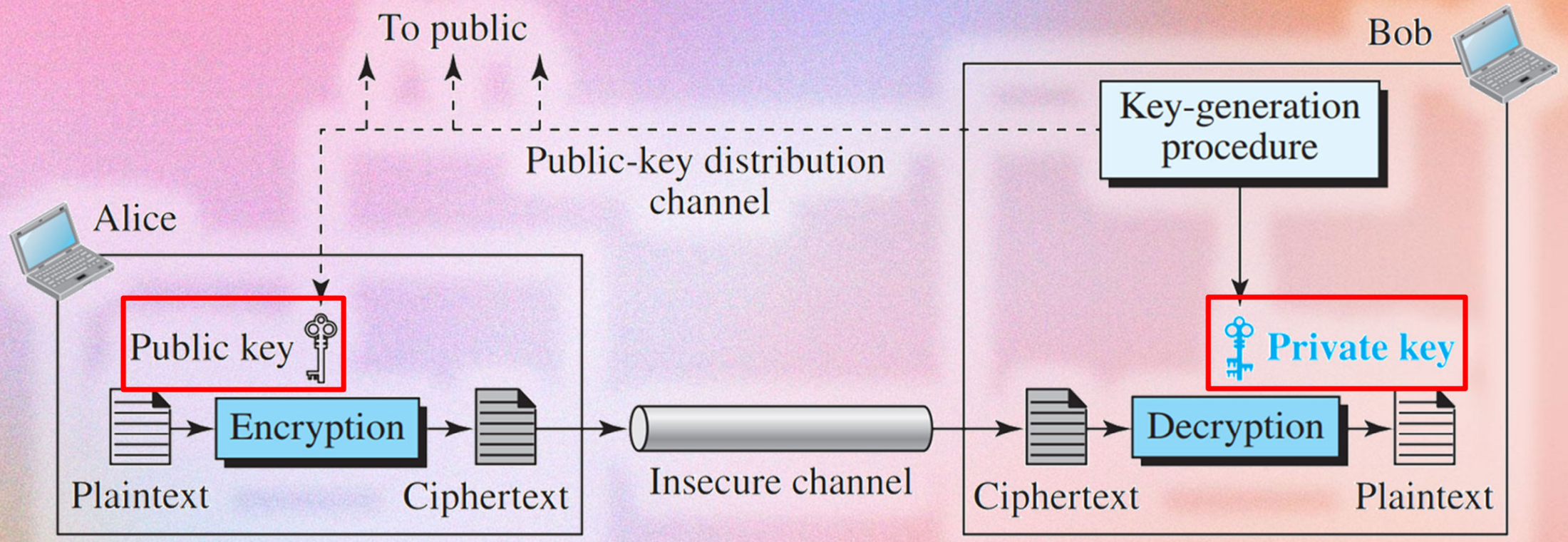
https://www.cs.utexas.edu/~byoung/cs361/lecture45.pdf

SYMMETRIC-KEY CIPHER



SYMMETRIC-KEY CIPHER: *uses the same key for both encryption and decryption*

ASYMMETRIC-KEY CIPHER



ASYMMETRIC-KEY CIPHER: *uses the **public key** for encryption and the **private key** for decryption*

THANK YOU!

Content Curated by Pollux M. Rey