MODERN CRYPTOGRAPHY

FOR THIS UNIT...

01 MODERN CRYPTOGRAPHY

02 DATA ENCRYPTION STANDARD

03 ADVANCED ENCRYPTION STANDARD

01

WHAT IS MODERN CRYPTOGRAPHY?

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).

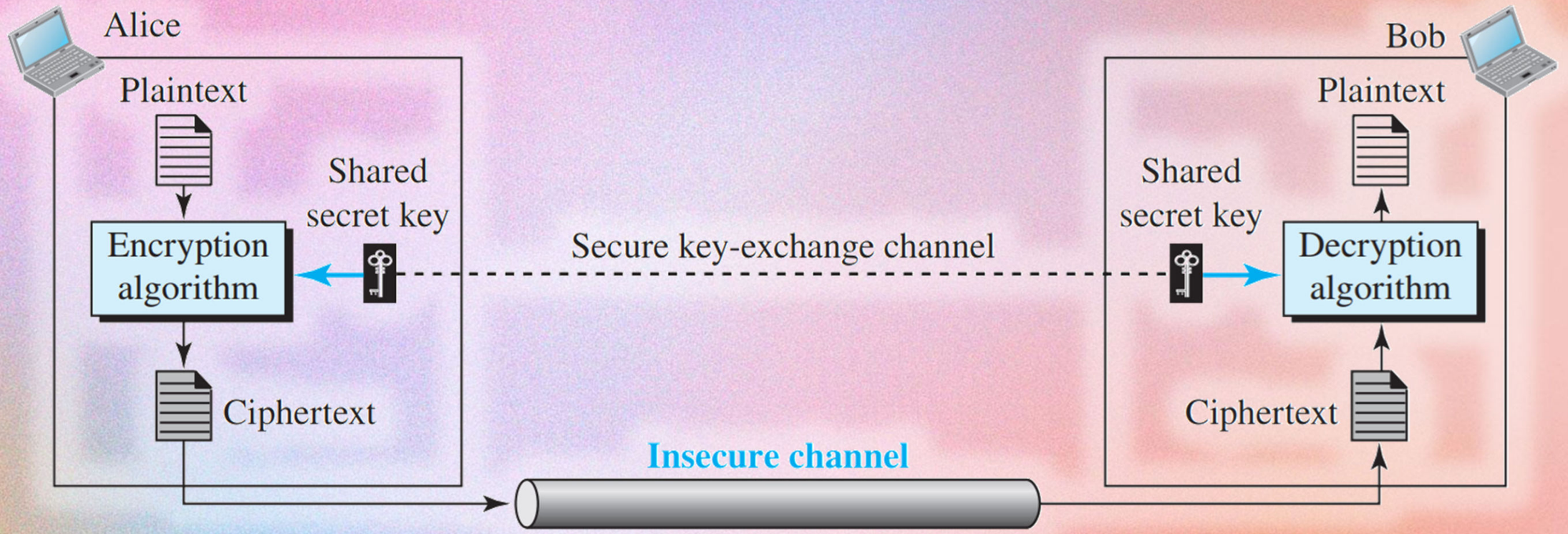
Cracking Codes with Python, Sweigrart
https://documents.uow.edu.au/~fuchun/book/Lecture1-PS.pdf
https://www.cse.iitd.ac.in/~siy107537/sil765/PDF/1-Provable-Security.pdf

02

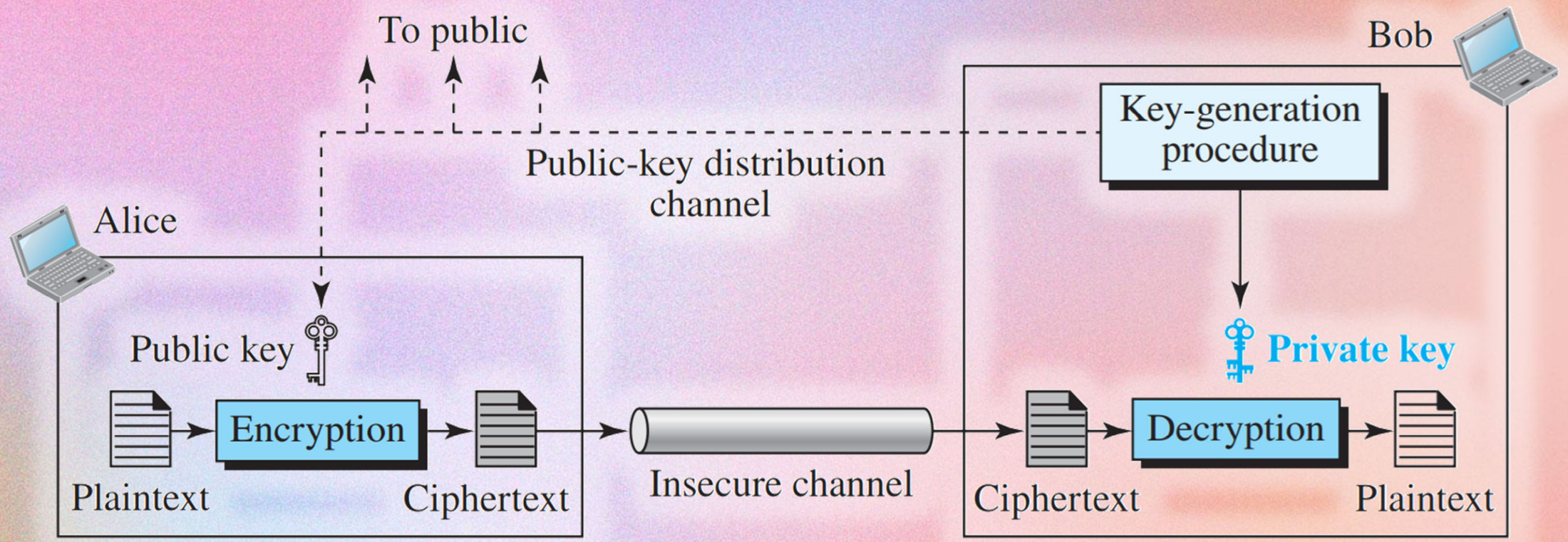
MODERN ENCRYPTION ALGORITHMS

Content Curated by Pollux M. Rey

SYMMETRIC-KEY CIPHER



ASYMMETRIC-KEY CIPHER



Data Encryption Standard

Advanced Encryption Standard

DATA ENCRYPTION STANDARD

An **early data encryption standard** endorsed by the U.S. National Bureau of Standards (now NIST) and **developed by IBM in the 1970s.**

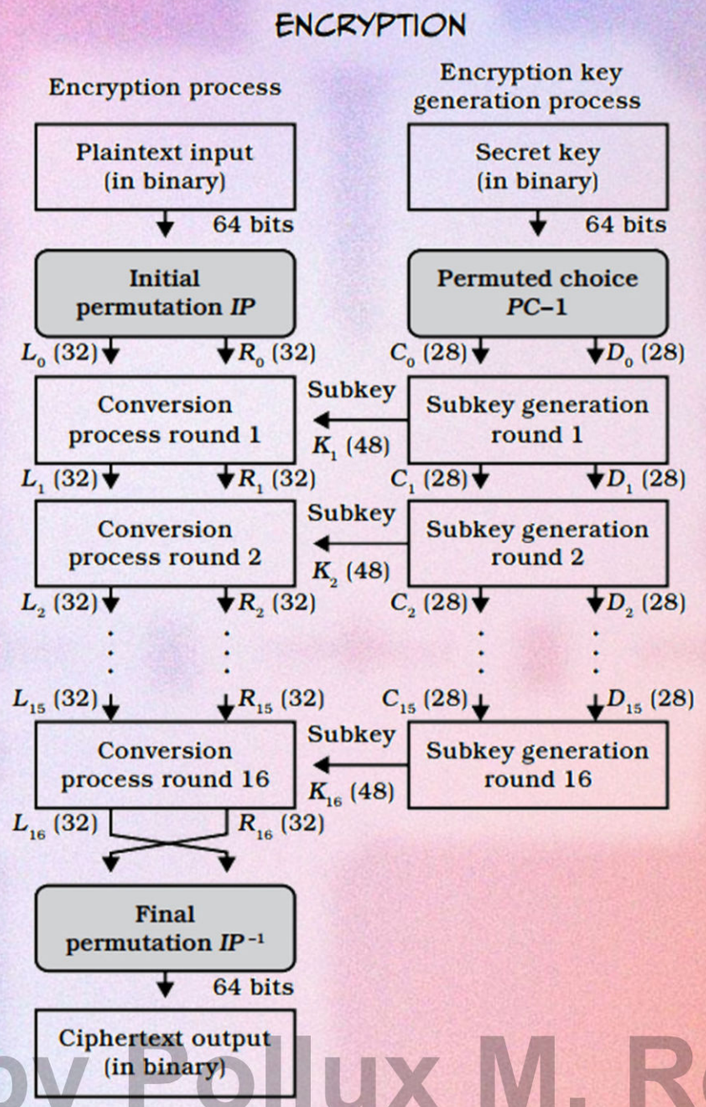
https://www.britannica.com/topic/Data-Encryption-Standard

DATA ENCRYPTION STANDARD

- It was based on IBM's patented **Lucifer algorithm**, developed by **Horst Feistel.**
- It was evaluated in secret consultations between the **NBS and the U.S. National Security Agency (NSA).**
- **Modifications included reducing the key size to 56 bits.**
- The final version of DES was **adopted as a federal standard in 1976 and published in 1977.**
- It was approved for use in **unclassified U.S. government applications.**
- DES also became widely used in **financial transactions, particularly in electronic fund transfers.**

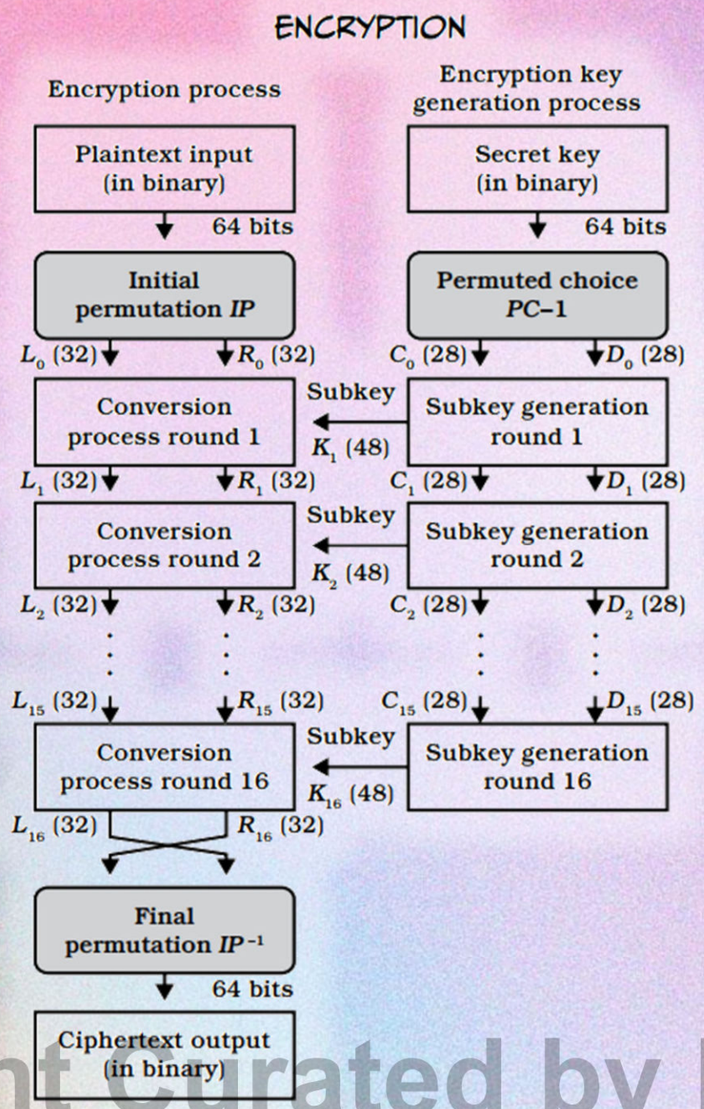
https://www.britannica.com/topic/Data-Encryption-Standard

DATA ENCRYPTION STANDARD



The Manga Guide to Cryptography, Mitani, Sato, Hinoki

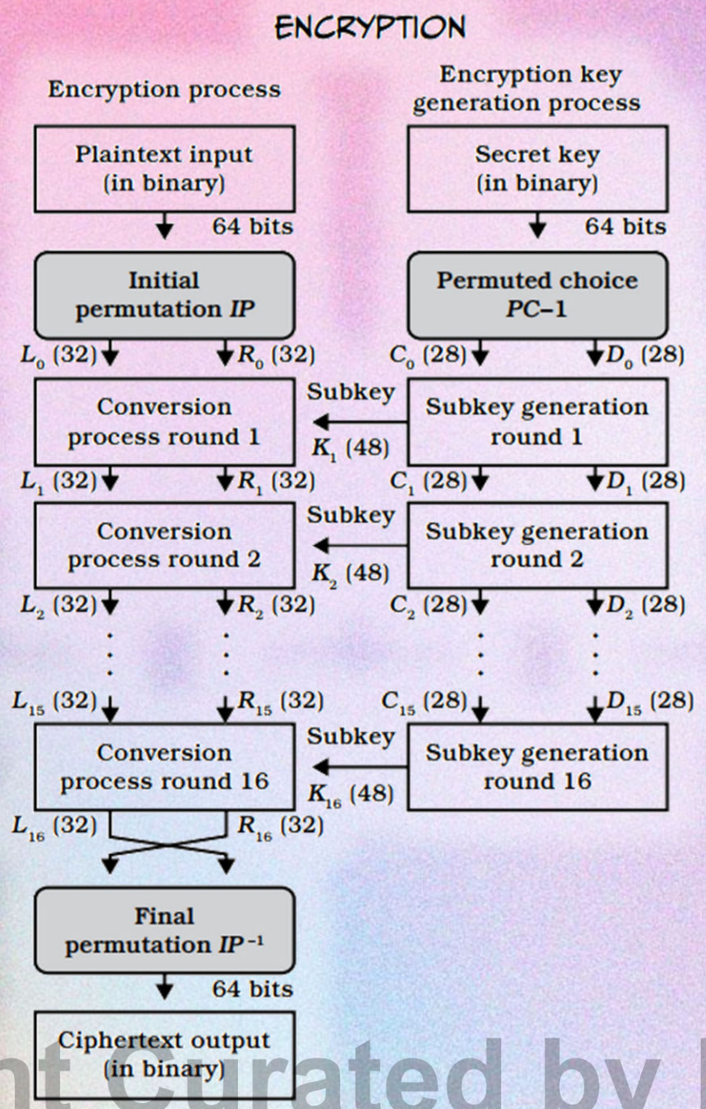
DATA ENCRYPTION STANDARD



It is a **product block cipher.**

https://www.britannica.com/topic/Data-Encryption-Standard

DATA ENCRYPTION STANDARD

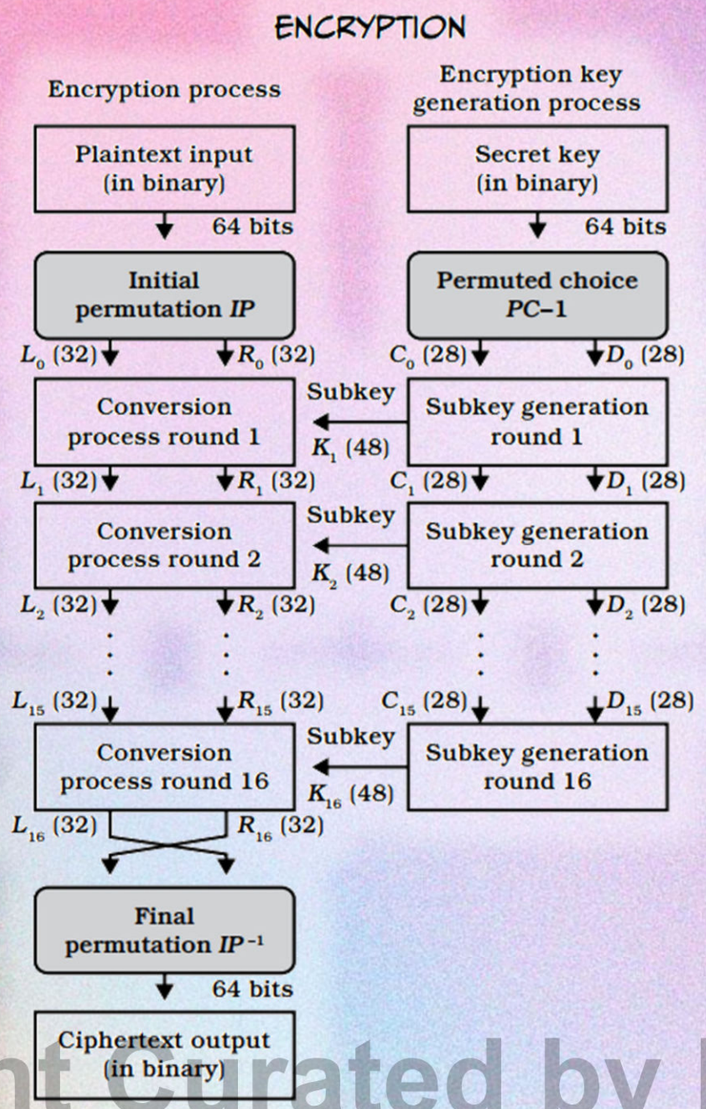


Product Cipher

Combining **multiple transposition or substitution ciphers**, which may result in **a more secure encryption.**

https://www.britannica.com/topic/product-cipher

DATA ENCRYPTION STANDARD

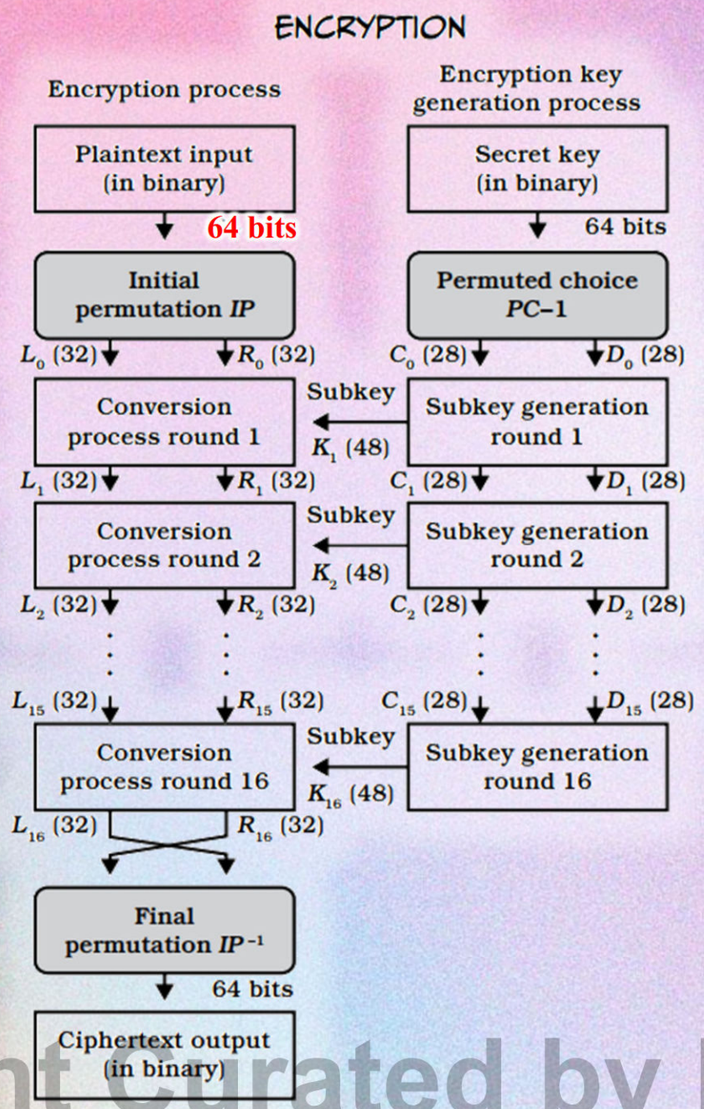


Block Cipher

Breaks the plaintext **into blocks of the same size** for encryption **using a common key.**

https://www.britannica.com/topic/cryptology/Secret-sharing

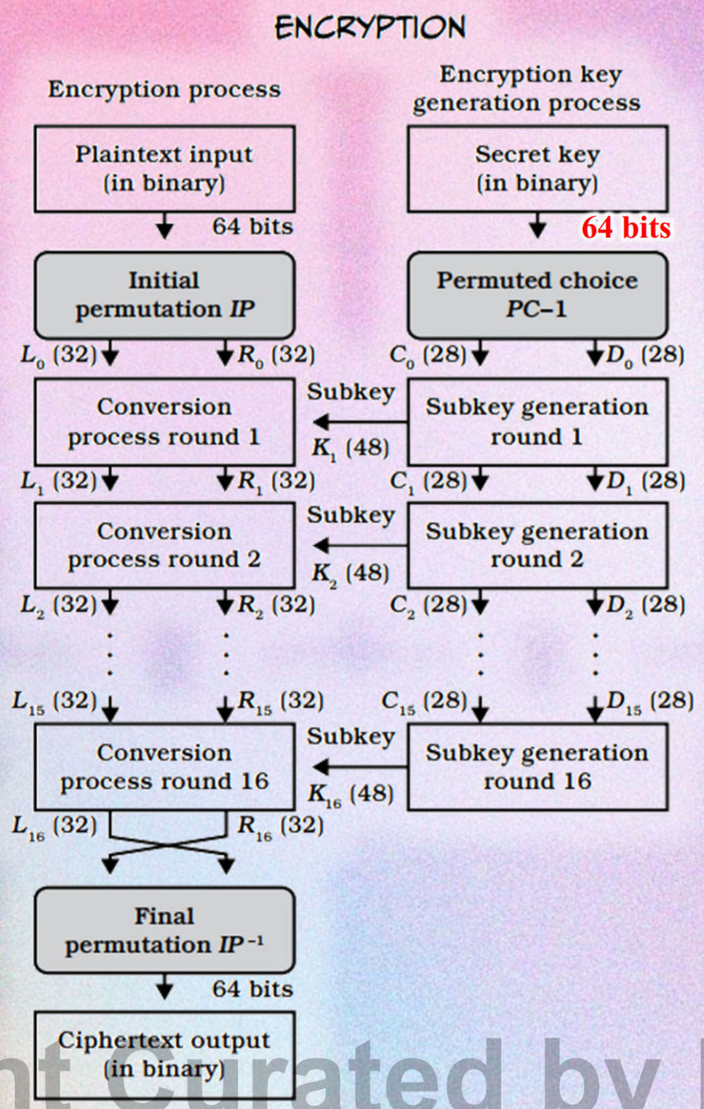
DATA ENCRYPTION STANDARD



The **block size** is **64 bits.**

https://www.britannica.com/topic/Data-Encryption-Standard

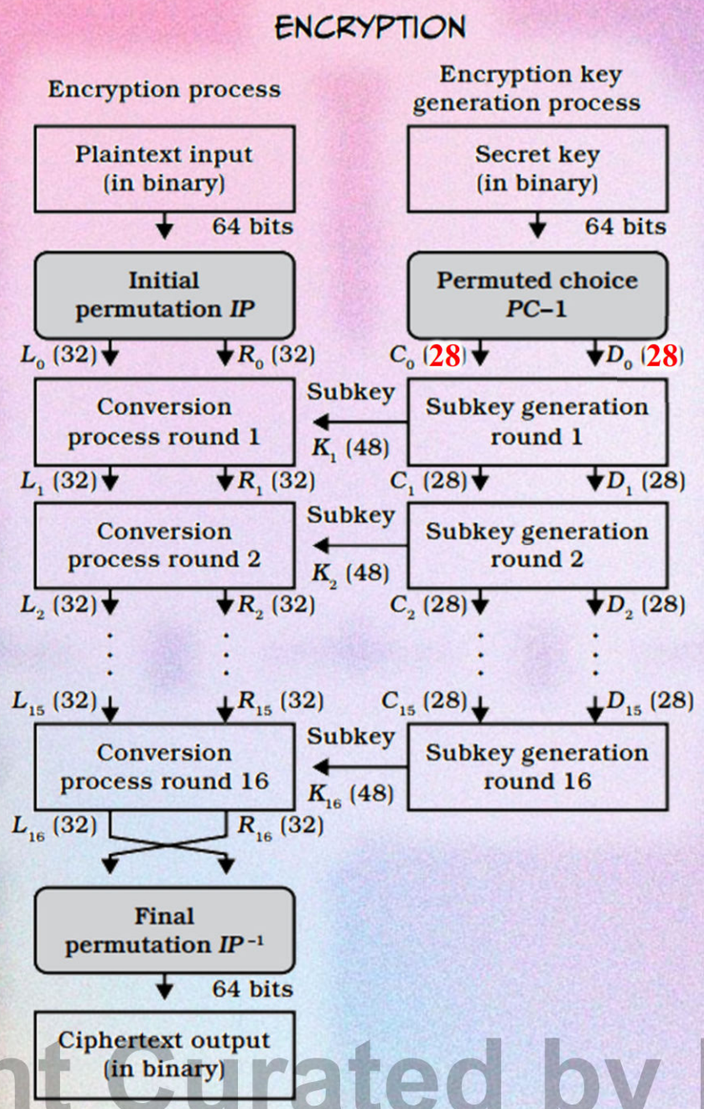
DATA ENCRYPTION STANDARD



The **key size** is **64 bits.**

https://www.britannica.com/topic/Data-Encryption-Standard

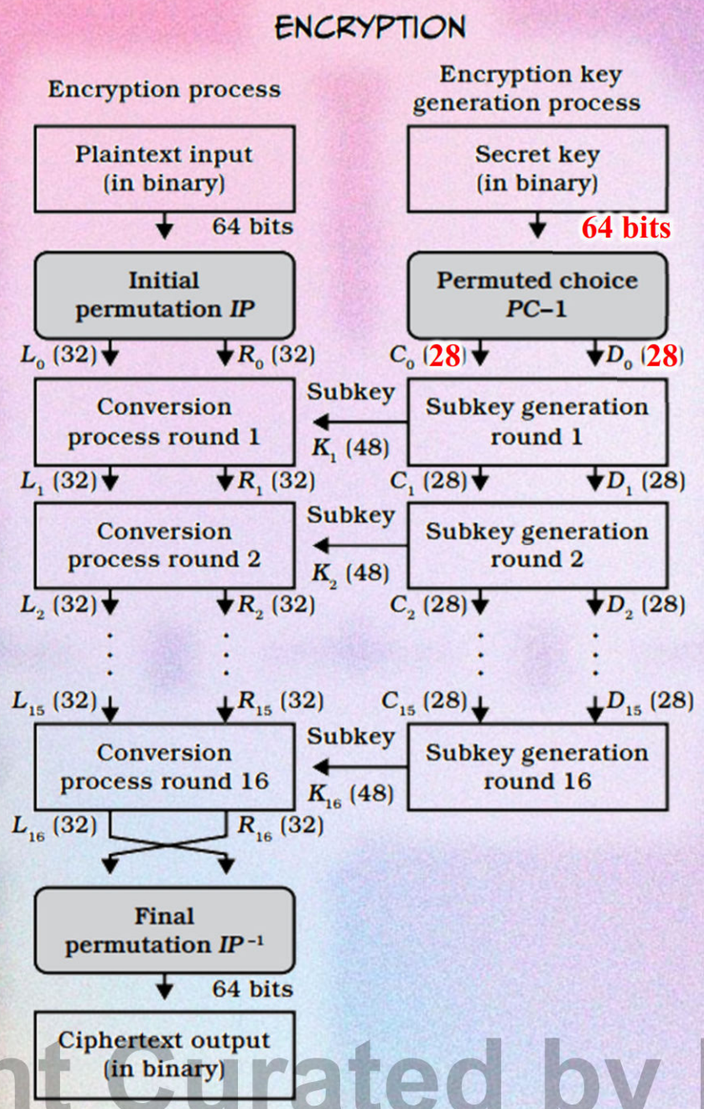
DATA ENCRYPTION STANDARD



Only 56 are actually key bits.

https://www.britannica.com/topic/Data-Encryption-Standard

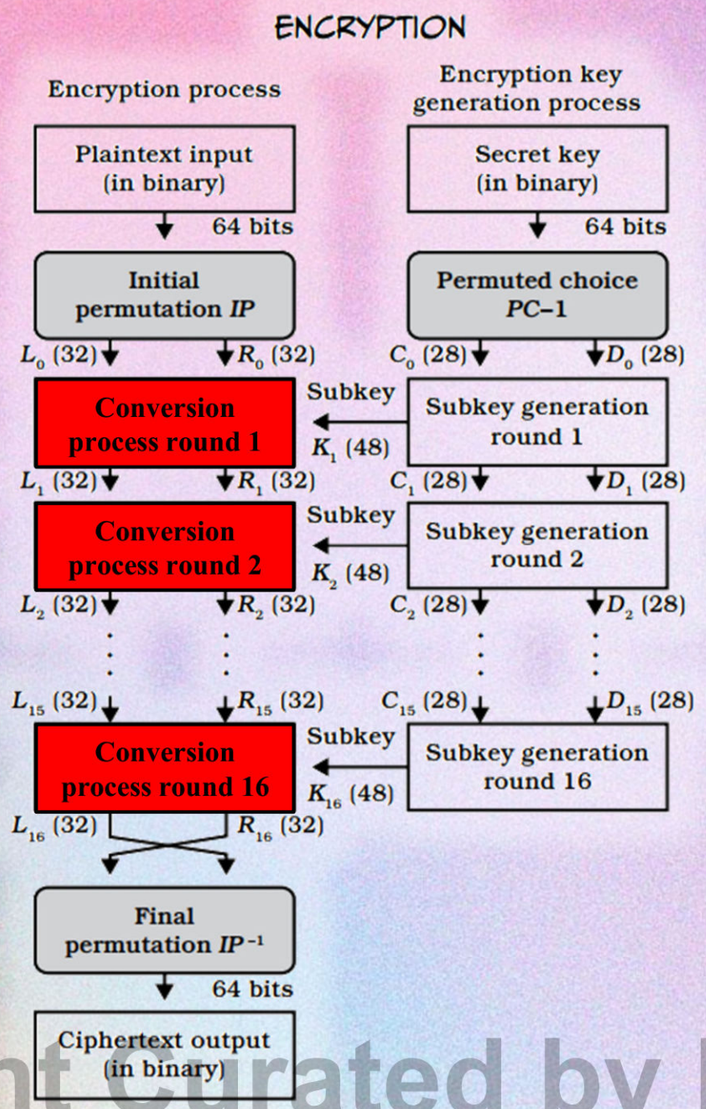
DATA ENCRYPTION STANDARD



The **remaining 8** are **parity check bits.**

https://www.britannica.com/topic/Data-Encryption-Standard

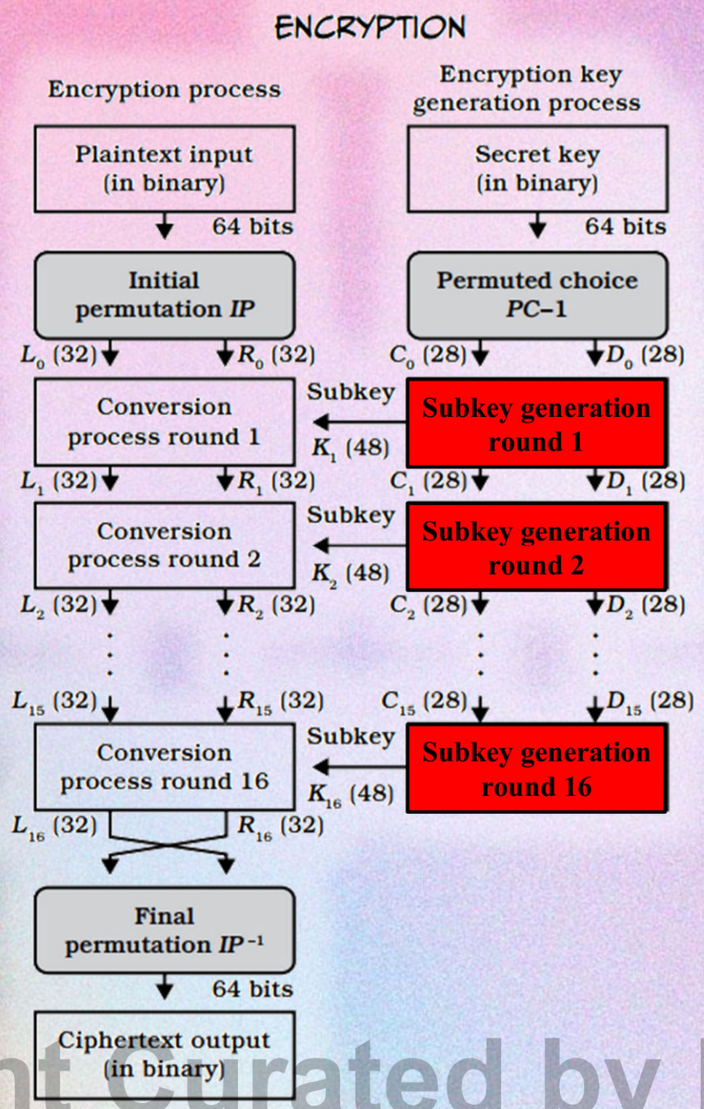
DATA ENCRYPTION STANDARD



It consists of **16 rounds** of **substitution and transposition.**

https://www.britannica.com/topic/Data-Encryption-Standard

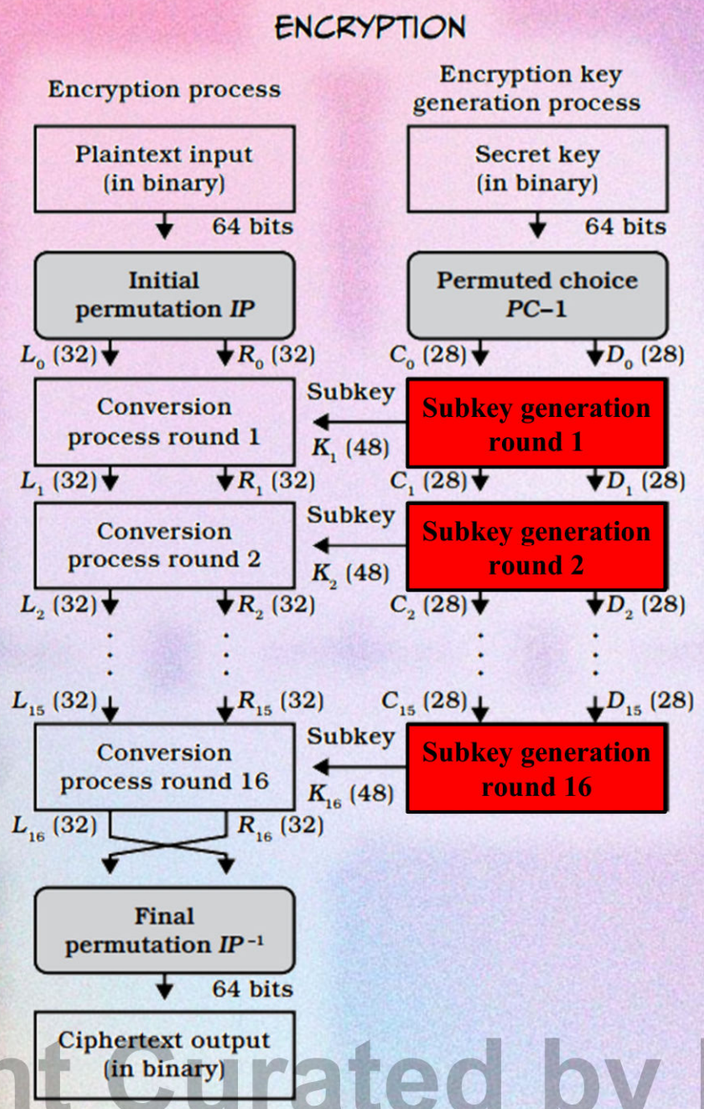
DATA ENCRYPTION STANDARD



Each round uses a **48-bit subkey.**

https://www.britannica.com/topic/Data-Encryption-Standard

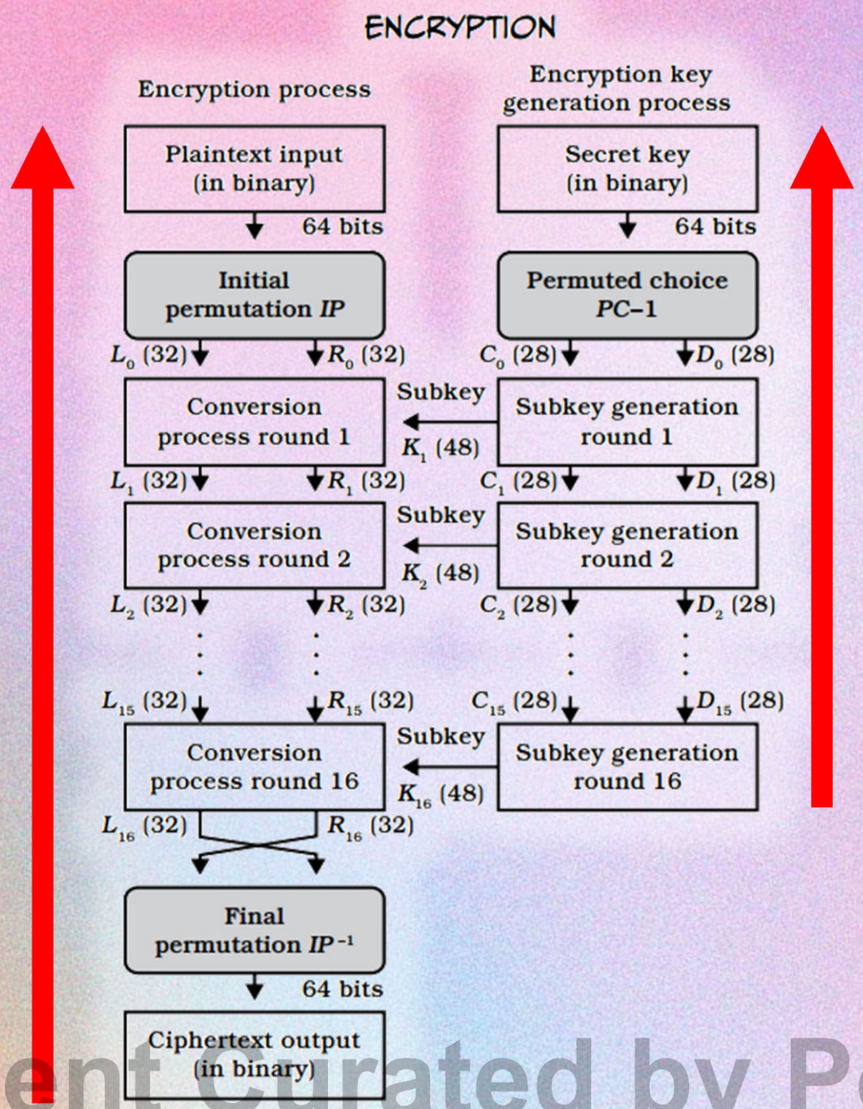
DATA ENCRYPTION STANDARD



These subkeys are also **used for encrypting other blocks.**

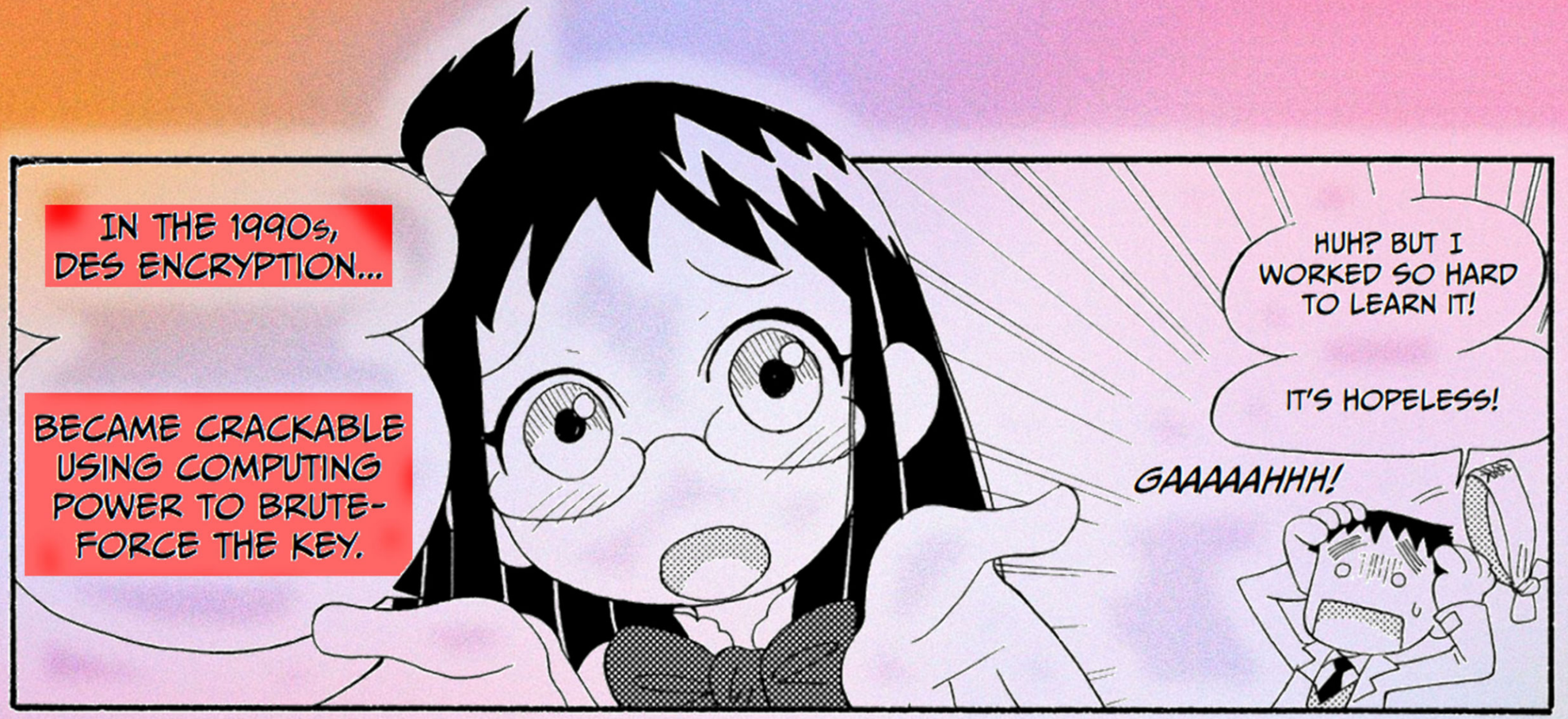
https://www.britannica.com/topic/Data-Encryption-Standard

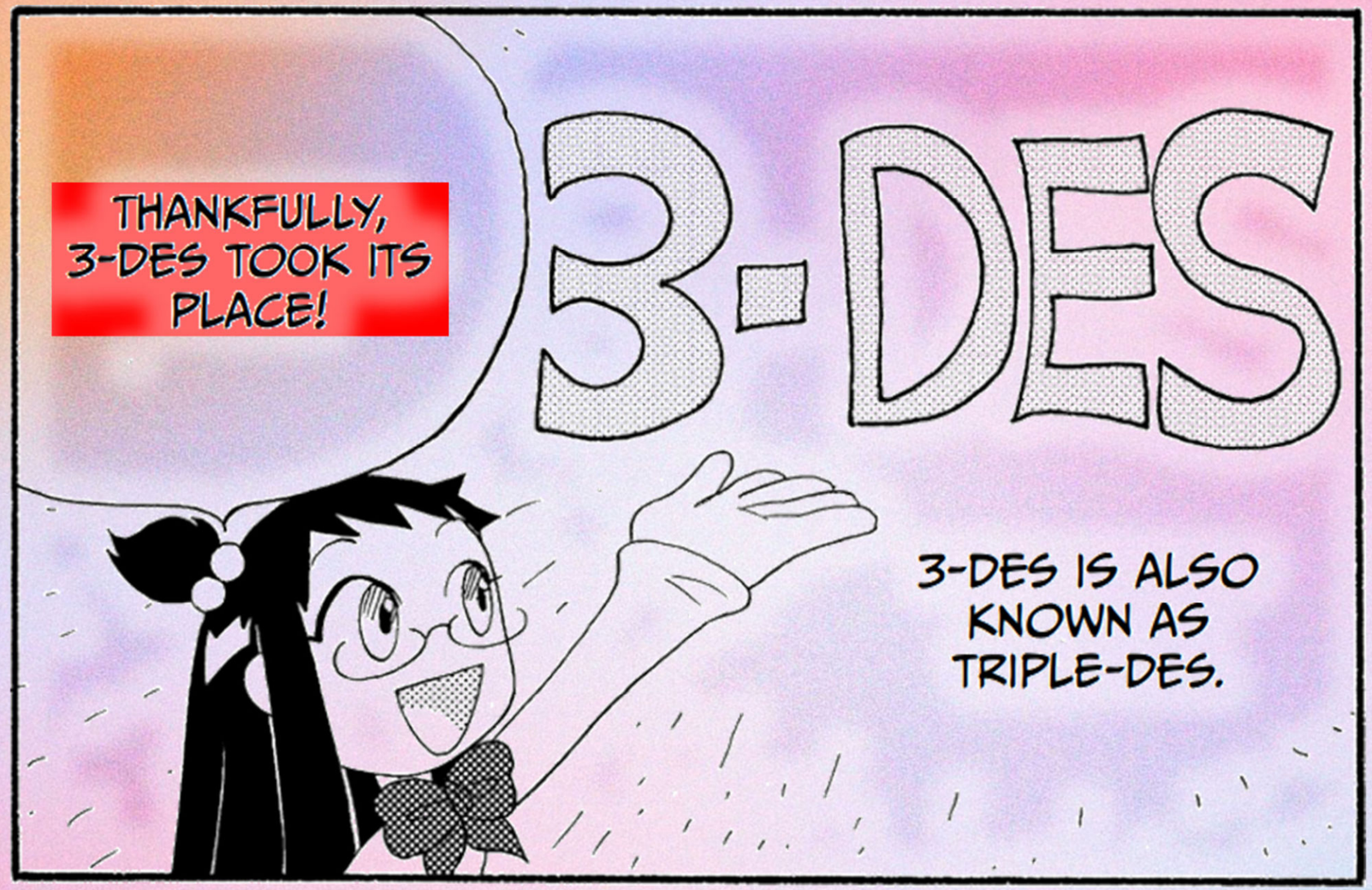
DATA ENCRYPTION STANDARD

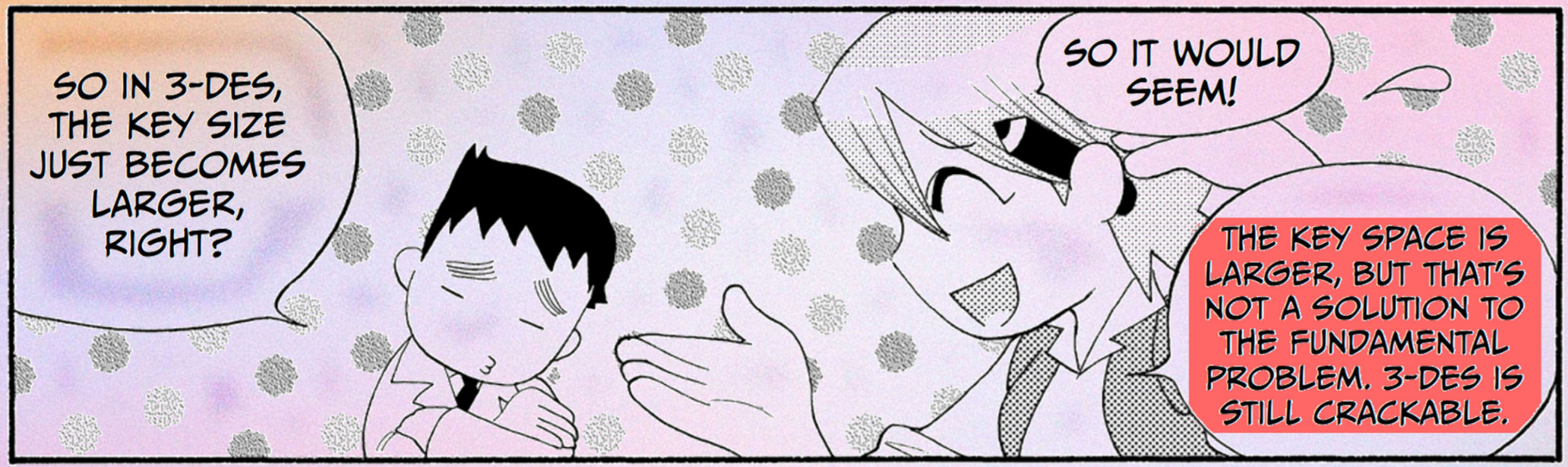


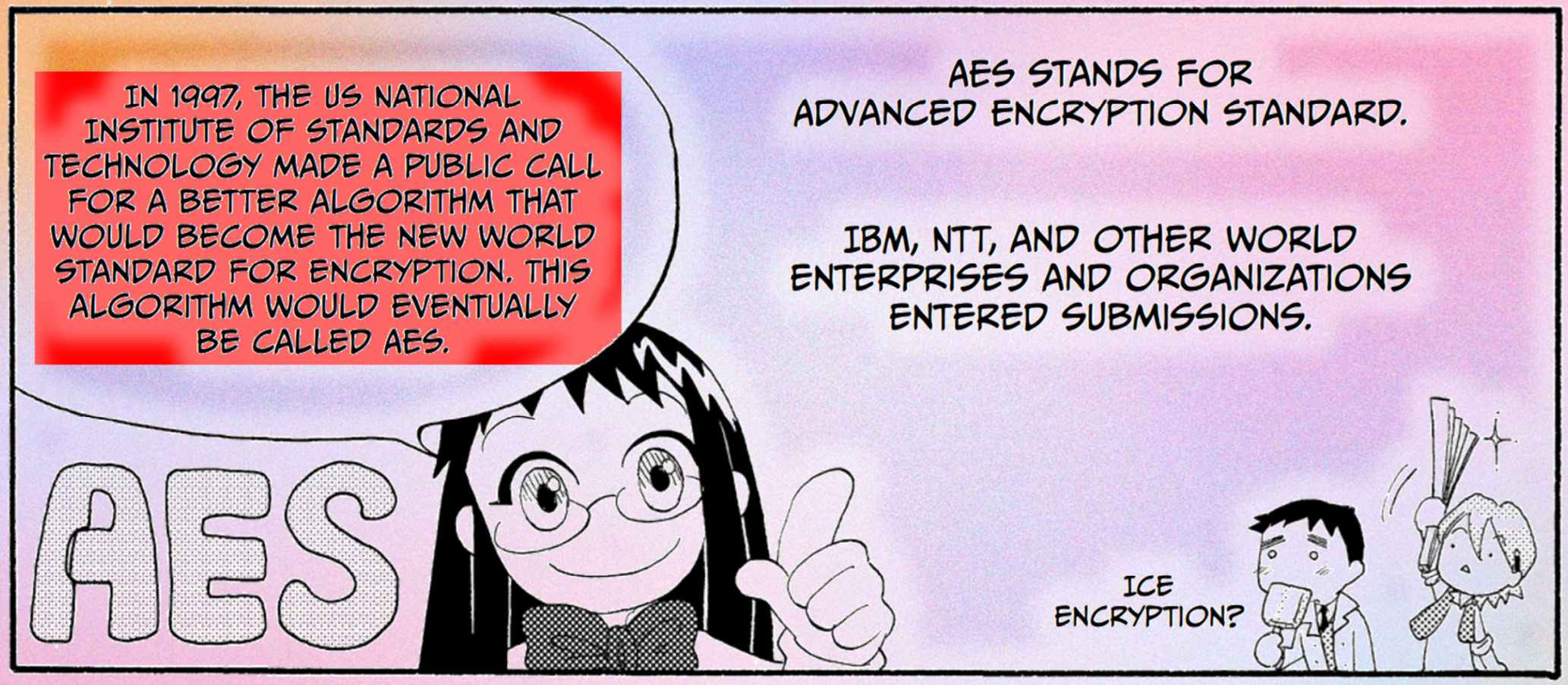
The **decryption process** is the **reverse order.**

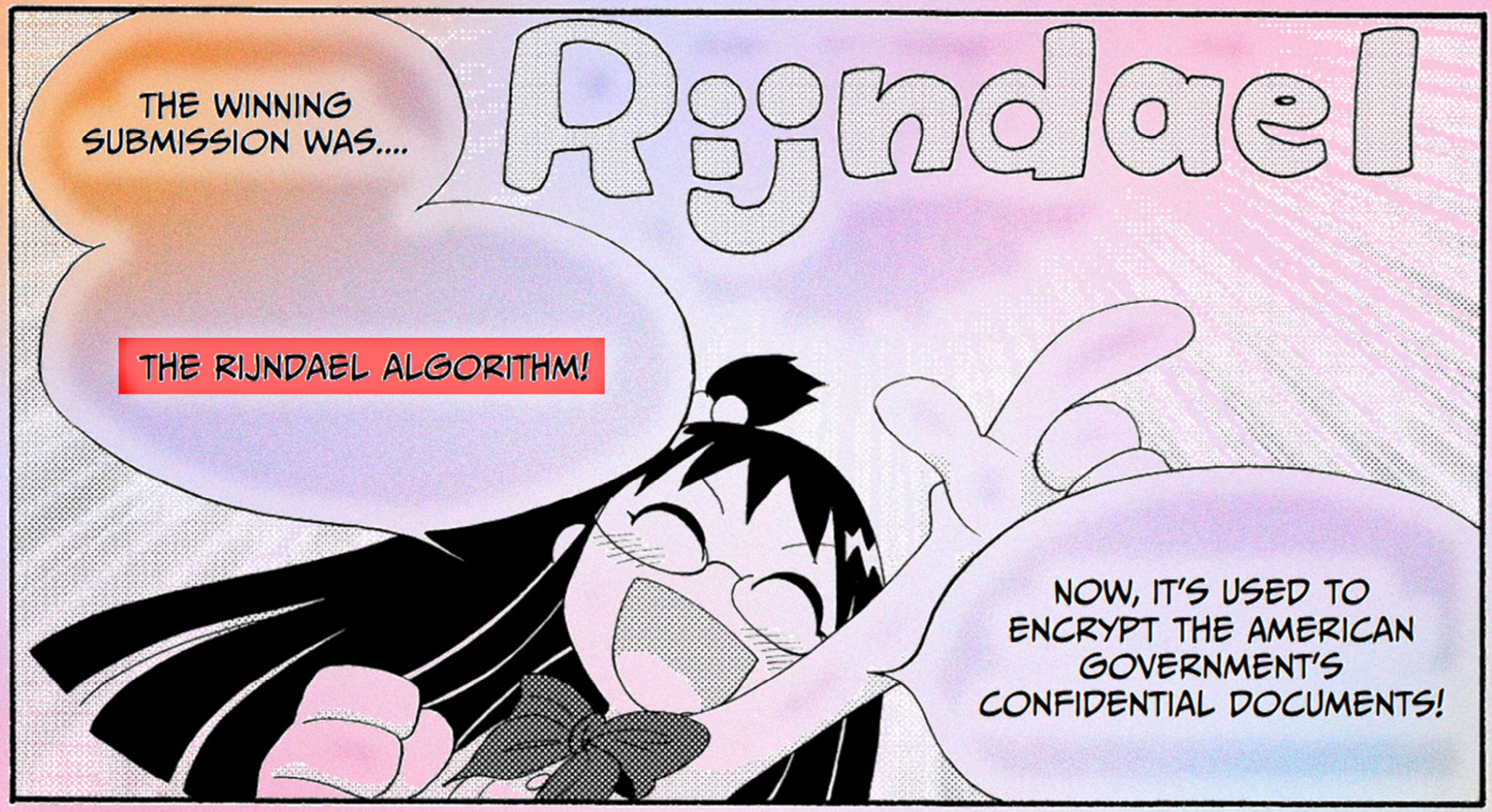
https://www.britannica.com/topic/Data-Encryption-Standard











The Manga Guide to Cryptography, Mitani, Sato, Hinoki

ADVANCED ENCRYPTION STANDARD

- Originally called the **Rijndael algorithm.**
- Developed by Belgian cryptographers **Joan Daemen and Vincent Rijmen.**
- Selected from 15 submissions across 12 countries to replace DES.

The Manga Guide to Cryptography, Mitani, Sato, Hinoki

ADVANCED ENCRYPTION STANDARD

Unlike DES, which has a fixed key size, **AES supports multiple key lengths** for enhanced security.

https://www.britannica.com/topic/AES

ADVANCED ENCRYPTION STANDARD

Type	Key Size (bits)	Block Size (bits)	Number of Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

The Manga Guide to Cryptography, Mitani, Sato, Hinoki

ADVANCED ENCRYPTION STANDARD

Type	Key Size (bits)	Block Size (bits)	Number of Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

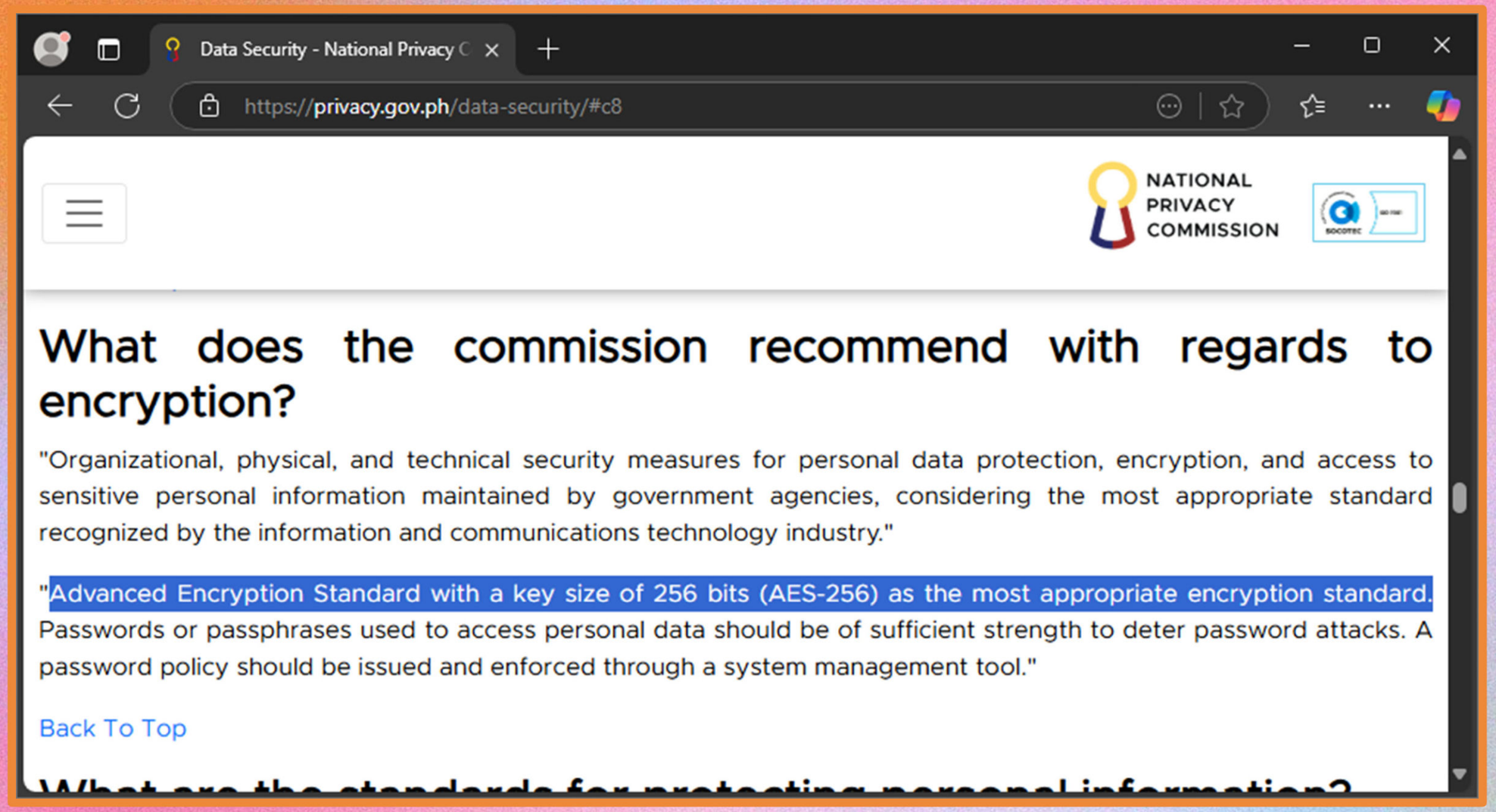
The Manga Guide to Cryptography, Mitani, Sato, Hinoki

The Manga Guide to Cryptography, Mitani, Sato, Hinoki

ADVANCED ENCRYPTION STANDARD

"Based on the DES experience, ***there is every reason to believe the AES will not succumb to cryptanalysis, nor will it be overrun by developments in computing****, as was the DES, since* ***its work factor can easily be adjusted to outpace them.***"

https://www.britannica.com/topic/AES



Content Curated by Pollux M. Rey

https://privacy.gov.ph/data-security/#c8

BLOCK CIPHER MODES OF OPERATION

NIST Special Publication 800-38A
2001 Edition

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendation for Block Cipher Modes of Operation

Methods and Techniques

Morris Dworkin

COMPUTER SECURITY

MODE OF OPERATION

A **technique for enhancing the effect of a cryptographic algorithm** or adapting the algorithm for an application.

Cryptography and Network Security, Stallings

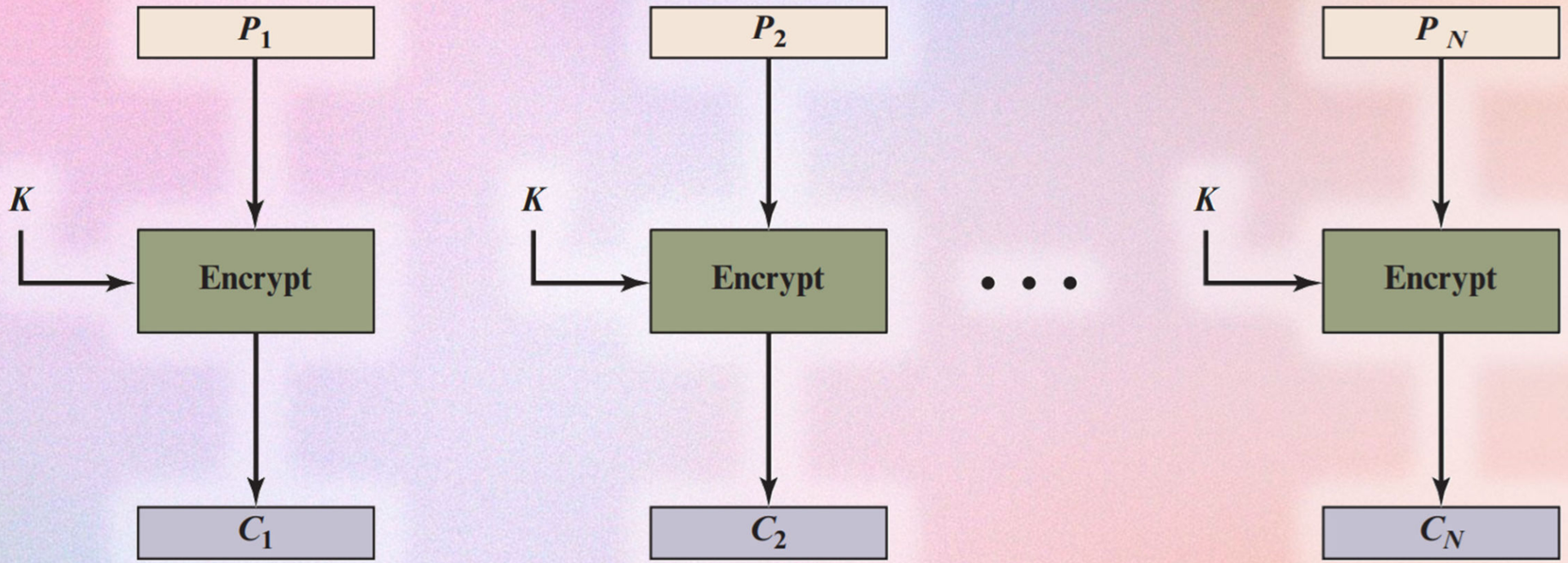
BLOCK CIPHER MODES OF OPERATION

Abstract

This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). Used with an underlying block cipher algorithm that is approved in a Federal Information Processing Standard (FIPS), these modes can provide cryptographic protection for sensitive, but unclassified, computer data.

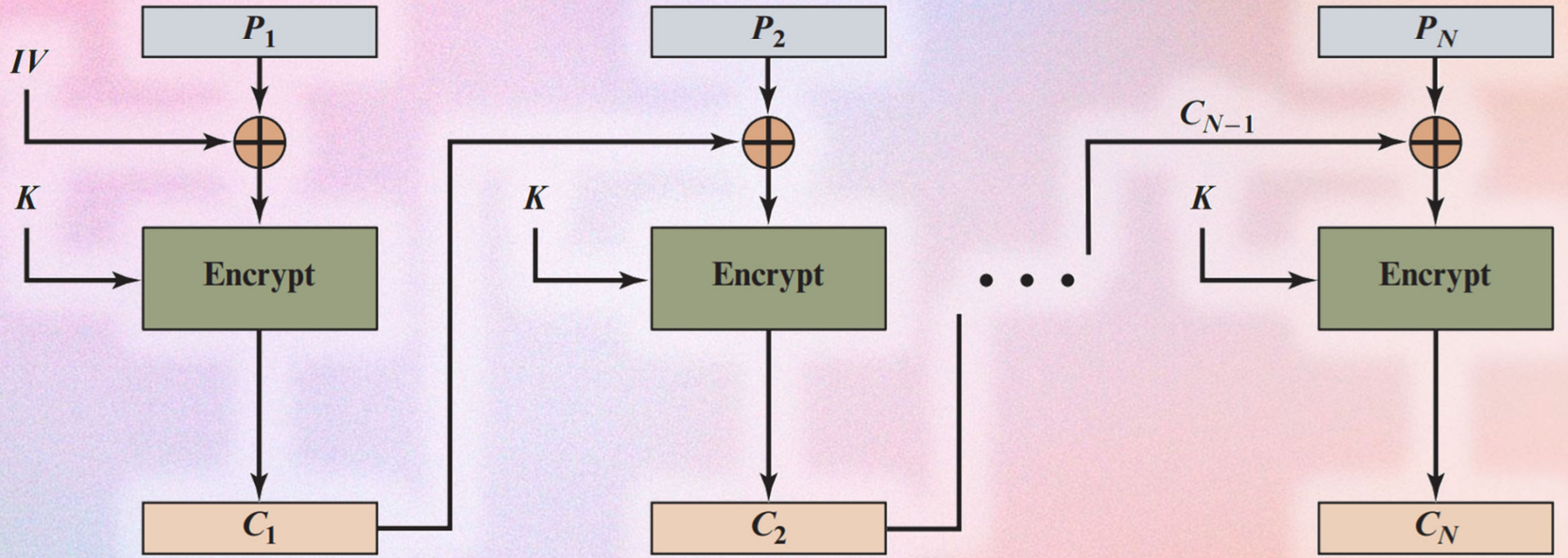
National Institute of Standards and Technology

ELECTRONIC CODEBOOK (ECB)



*Each block of plaintext bits is **encoded independently** using the same key.*

CIPHER BLOCK CHAINING (CBC)



The input to the encryption algorithm is the ***XOR of the next block of plaintext and the preceding block of ciphertext.***

ADVANCED ENCRYPTION STANDARD

Federal Information

Processing Standards Publication 197

Published: November 26, 2001
Updated: May 9, 2023

Announcing the
ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS) are developed by NIST under 15 U.S.C. 278g-3 and issued by the Secretary of Commerce under 40 U.S.C. 11331.

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS 197).
2. **Category of Standard.** Computer Security Standard, Cryptography.
3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) digital information.

PRINCIPLES OF MODERN CRYPTOGRAPHY

"Modern cryptographers emphasize that ***security should not depend on the secrecy of the encryption method (or algorithm), only the secrecy of the keys.***"

https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html

SYMMETRIC-KEY CRYPTOGRAPHY

SYMMETRIC-KEY CRYPTOGRAPHY

DIFFIE-HELLMAN KEY EXCHANGE

It is used to **establish a secure communication channel.**

DIFFIE-HELLMAN KEY EXCHANGE

This **channel** is used by the systems to **exchange a private key.**

DIFFIE-HELLMAN KEY EXCHANGE

This **private key** is then **used to do symmetric encryption between the two systems.**

DIFFIE-HELLMAN KEY EXCHANGE

Agree upon two numbers:

P Prime Number 13

G Generator of P 6

Private = 5

Randomly generate a Private Key

Private = 4

(6^{5}) MOD 13

(7776) MOD 13

Public = 2

Calculate Public Key:

$(G^{Private})$ MOD P

(6^{4}) MOD 13

(1296) MOD 13

Public = 9

Exchange Public Keys

(9^{5}) MOD 13

(59049) MOD 13

Shared Secret = 3

Calculate the Shared Secret

$(Shared\ Public^{Private})$ MOD P

(2^{4}) MOD 13

(16) MOD 13

Shared Secret = 3

PRACTICAL NETWORKING .NET

DIFFIE-HELLMAN KEY EXCHANGE

MODERN ASYMMETRIC-KEY CIPHERS

RSA

ECC

Diffie and Hellman's paper **introduced a new cryptographic approach** and challenged experts to **develop a public-key algorithm.**

Cryptography and Network Security, Stallings

One of the **first successful responses to the challenge** was the **RSA algorithm**, which was developed in 1977 by **Ron Rivest, Adi Shamir, and Len Adleman** at MIT.

RSA ALGORITHM

It is the world's **first public-key encryption system**, where its strength lies in the **difficulty of factoring large integers (semiprimes).**

The Manga Guide to Cryptography, Mitani, Sato, Hinoki

r/crypto • 8 yr. ago
markannen

Why is it hard to factor large numbers?

9 | 51 | Share

[deleted] • 8y ago

The short answer is that there's no mathematical trick to finding f the factors. The only way to do it is trial and error until you find the answer. Blindly guessing prime factors until you find two that give you the right product.

Interestingly, it's not actually *proven* to be an NP-hard problem. There may be a trick to it that isn't publicly known.

8 | Award | Share | ...

https://www.reddit.com/r/crypto/comments/5gz1l8/comment/dawevge/

$$3 \times 11 = 33$$

34905295108476509491478496199038981334177646384933878439908205 77

×

32769132993266709549961988190834461413177642967992942539798288533

=

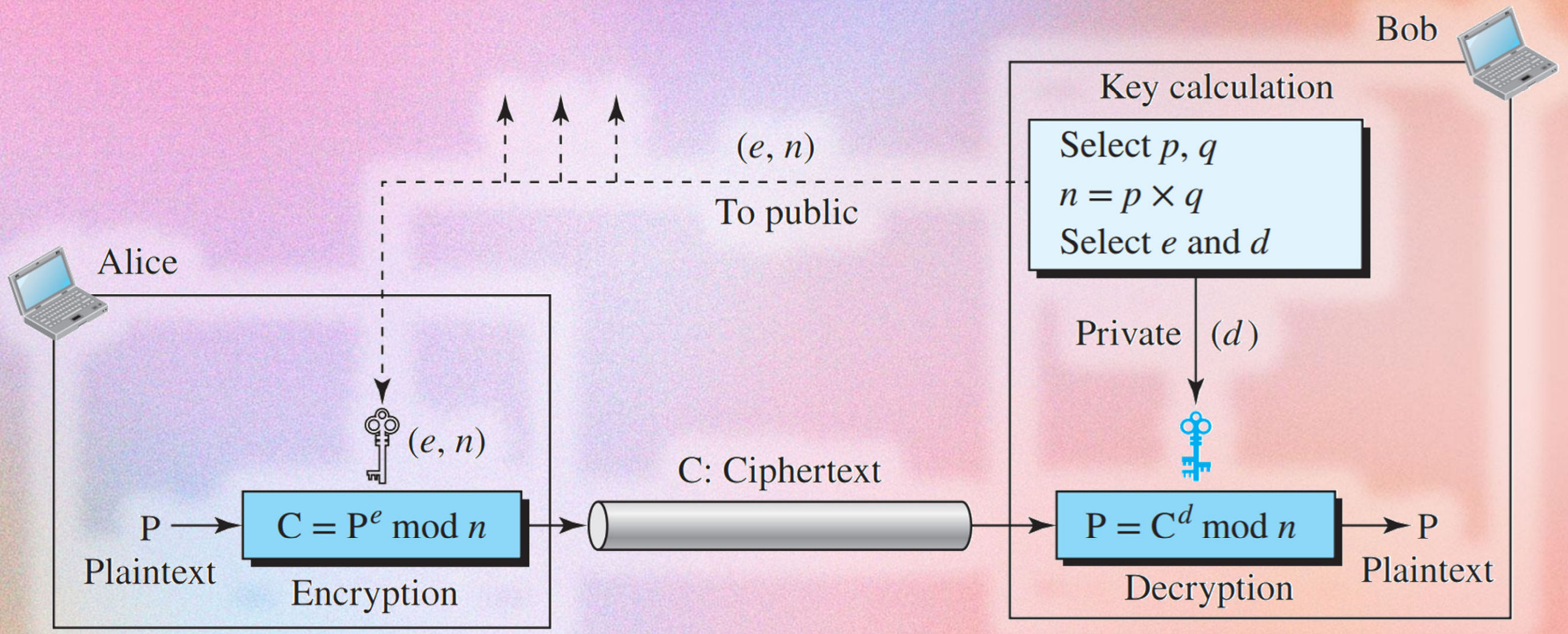
1143816257578888676692357799761466120102182967212423625625618429357069352457338978305971235639587050589890751475992900268795435 41

"The Magic Words are Squeamish Ossifrage"

Content Curated by Pollux M. Rey

The Manga Guide to Cryptography, Mitani, Sato, Hinoki

RSA ALGORITHM



RSA ALGORITHM

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Cryptography and Network Security, Stallings

RSA ALGORITHM

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

RSA ALGORITHM

Decryption by Alice with Alice's Private Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

RSA ALGORITHM

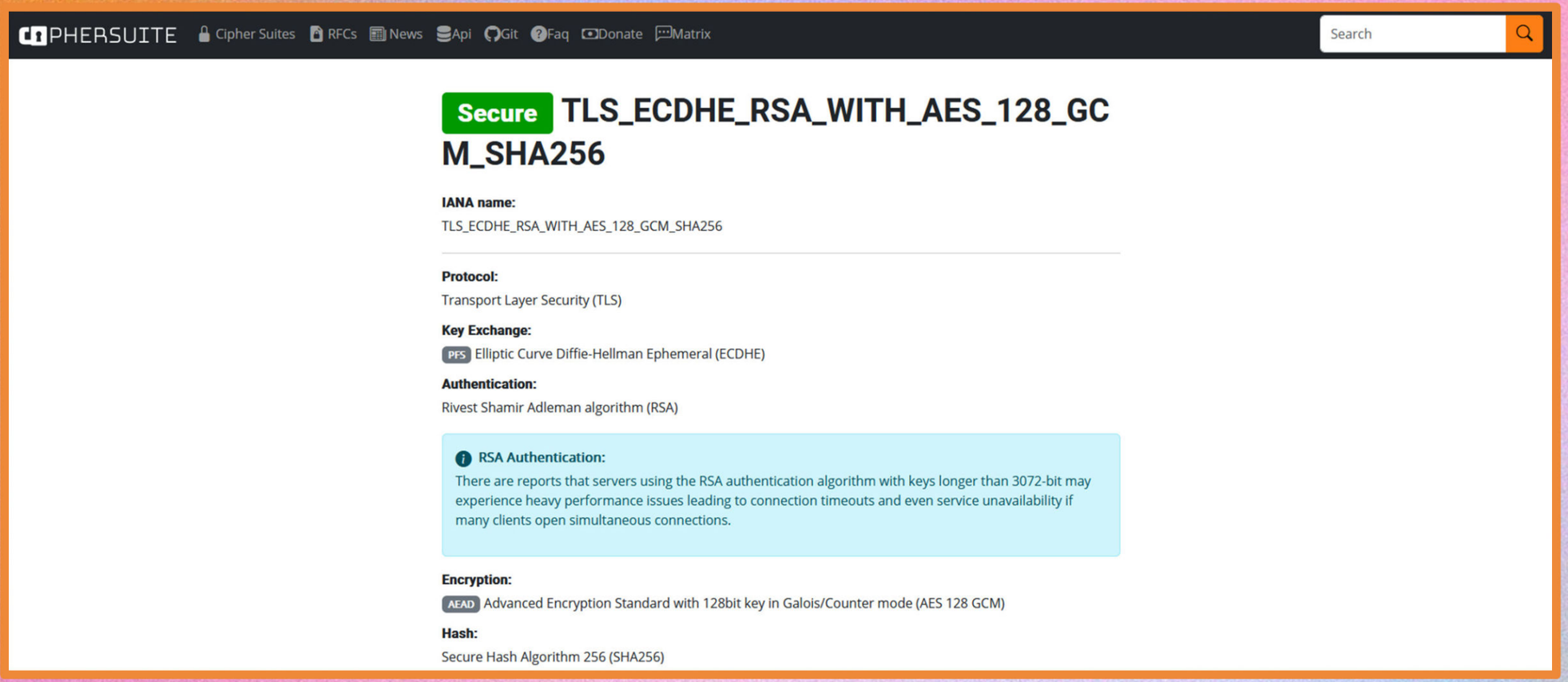
Although RSA can be used to encrypt and decrypt actual messages, it is **very slow if the message is long. RSA, therefore, is useful for short messages.**

RSA ALGORITHM

In fact, RSA is widely used in **digital signatures.**

A **digital signature** is an **electronic, encrypted, stamp of authentication** on **digital information.**

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



#StopRansomware: MedusaLocker

Technical Details

MedusaLocker ransomware actors most often gain access to victim devices through vulnerable Remote Desktop Protocol (RDP) configurations [T1133]. Actors also frequently use email phishing and spam email campaigns—directly attaching the ransomware to the email—as initial intrusion vectors [T1566].

MedusaLocker ransomware uses a batch file to execute PowerShell script `invoke-ReflectivePEInjection` [T1059.001]. This script propagates MedusaLocker throughout the network by editing the `EnableLinkedConnections` value within the infected machine's registry, which then allows the infected machine to detect attached hosts and networks via Internet Control Message Protocol (ICMP) and to detect shared storage via Server Message Block (SMB) Protocol.

MedusaLocker then:

- Restarts the `LanmanWorkstation` service, which allows registry edits to take effect.
- Kills the processes of well-known security, accounting, and forensic software.
- Restarts the machine in safe mode to avoid detection by security software [T1562.009].
- Encrypts victim files with the AES-256 encryption algorithm; the resulting key is then encrypted with an RSA-2048 public key [T1486].

PhilHealth
Your Partner in Health

BAGONG PILIPINAS

URGENT NOTICE TO THE PUBLIC

02 October 2023

On 22 September 2023, the Corporation suffered a cyberattack from the Medusa Ransomware which compromised the data stored from some of our servers and local workstations. The primary database was intact and not infected. The incident was immediately reported to the Department of Information and Communications Technology (DICT), the National Privacy Commission (NPC) in order to expediently resolve the matter; and to law enforcement agencies such as the Philippine National Police (PNP) Cybercrime Division, Cybercrime Investigation and Coordinating Center (CICC) and the National Bureau of Investigation (NBI) in order to identify and capture the perpetrators.

BLOG POST | DEC 02, 2024

The clock is ticking: NIST's bold move towards Post-Quantum Cryptography

NIST is driving the global transition to post-quantum cryptography, setting a 2030 deadline to deprecate RSA-2048 and ECC-256 algorithms and banning them entirely by 2035. This shift addresses quantum computing's potential to compromise current encryption, emphasizing the need for quantum-resistant solutions to combat risks like "harvest now, decrypt later" attacks. Organizations must act urgently, auditing systems and adopting post-quantum cryptographic algorithms to protect long-term data security. Collaborative efforts, such as shorter certificate lifespans and cloud-native solutions, are crucial for public and private systems to adapt effectively.

Contributor

Sectigo Team
Delivering Digital Trust

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash (A)	Hash (B)
				Key	Group			
Legacy [1]	80	2TDEA	1024	160	1024	160	SHA-1 [2]	
2019 - 2030	112	(3TDEA) [3] AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

After **RSA** and **Diffie-Hellman**, researchers started looking for **other cryptographic algorithms**, moving **beyond factoring.**

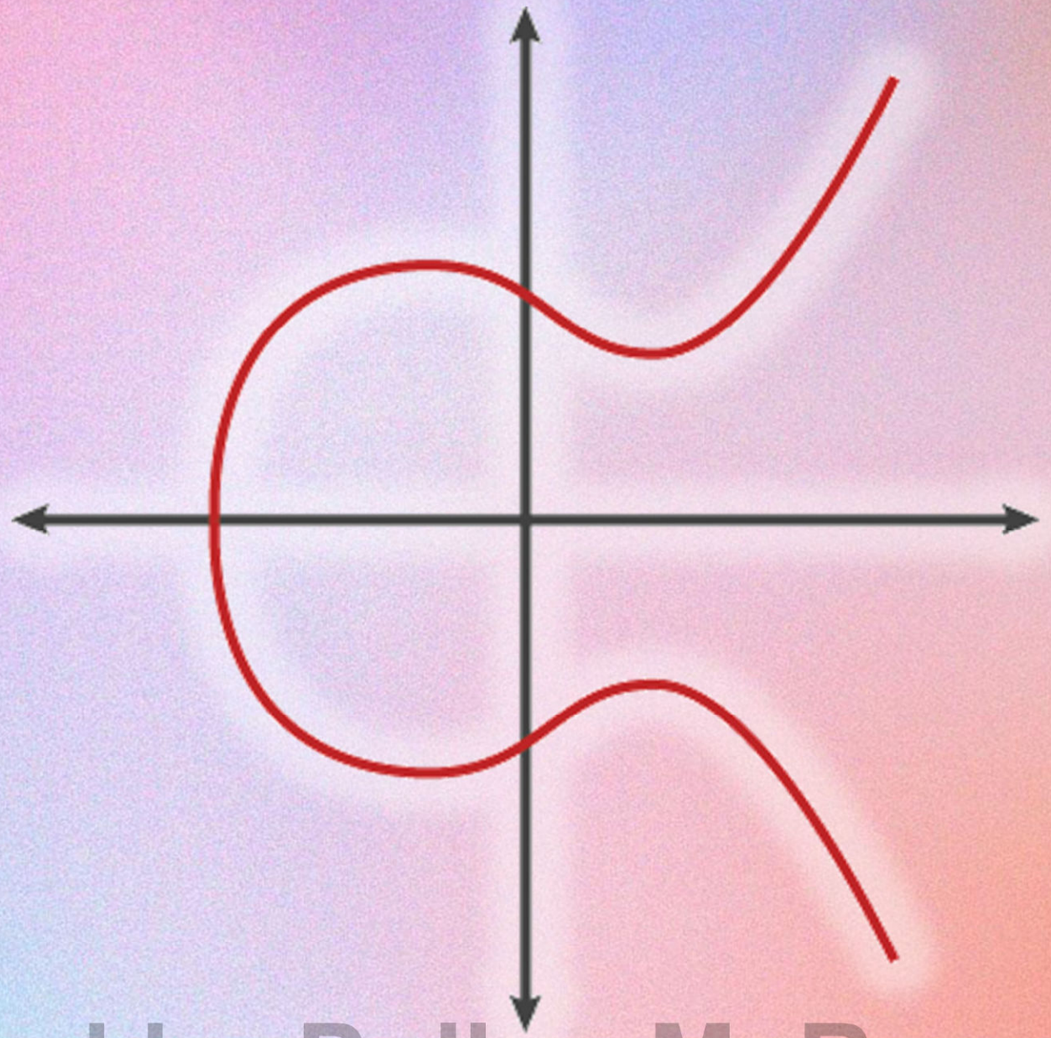
Serious Cryptography by Jean-Philippe Aumasson

ELLIPTIC CURVE CRYPTOGRAPHY

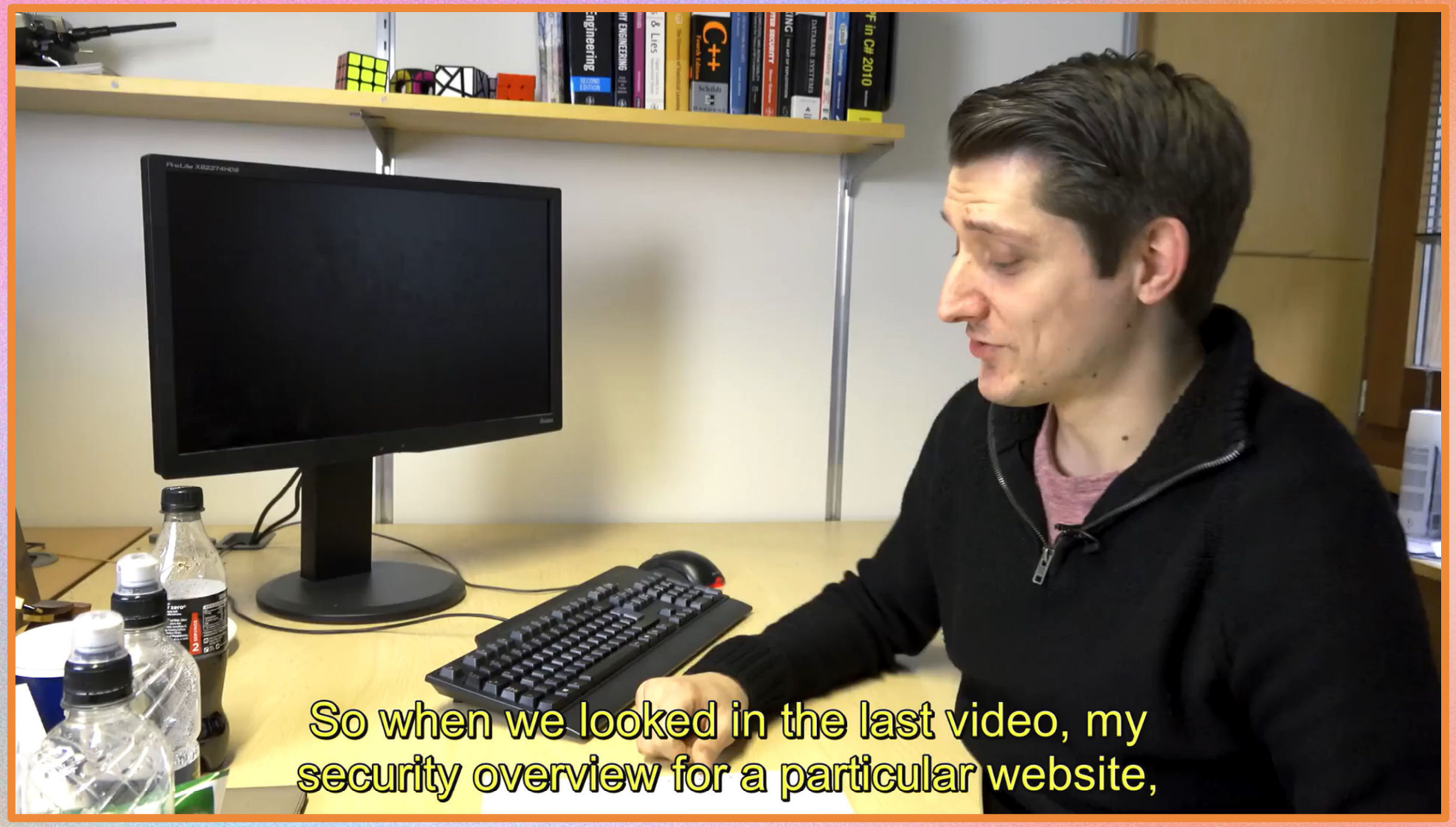
In **1985**, they proposed using elliptic curves as the basis for **elliptic curve cryptography (ECC).**

Serious Cryptography by Jean-Philippe Aumasson

ELLIPTIC CURVE



https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/



Content Curated by Pollux M. Rey

https://www.youtube.com/watch?v=NF1pwjL9-DE

SUMMARY

- **Elliptic Curve Cryptography (ECC)** is based on the equation $y^2=x^3+ax+b$.
- **ECC uses shorter key sizes** than RSA and Diffie-Hellman, making it **more efficient.**
- The **private key** is a number that determines **how many times a point moves along the curve.**
- The **public key** is the point on the curve, calculated by **multiplying a fixed point (known as the generator) by the private key.**

https://www.youtube.com/watch?v=NF1pwjL9-DE

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

https://www.keylength.com/

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes

Recommended TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

IANA name:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Protocol:

Transport Layer Security (TLS)

Key Exchange:

PFS Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)

Authentication:

Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption:

AEAD Advanced Encryption Standard with 256bit key in Galois/Counter mode (AES 256 GCM)

Hash:

Secure Hash Algorithm 384 (SHA384)

Elliptic curves allow you to **perform common public-key cryptography operations**, such as encryption, digital signatures, and key agreement, **faster than their classical counterparts.**

Serious Cryptography by Jean-Philippe Aumasson

THANK YOU!

Content Curated by Pollux M. Rey