

Introduction to Computer Security Lecture Slides

© 2024 by [Mihai Chiroiu](#) & [Florin Stancu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0
International](#)

Introduction to Cryptographic Systems

This lecture

- Is **not** about:
 - **Steganography**: the practice of concealing a file/message/image/video within another file/message/image/video.
 - **Obfuscation**: the practice of hiding the implementation of a program without altering its execution (Indistinguishability Obfuscation [9])
 - **Cryptocoins!!!**
- Is about:
 - Cryptography – the science of writing a secret message.
 - Cryptanalysis – the science of breaking cryptography.
 - Cryptology – all of the above (actually, synonymous with *cryptography*).

Vocabulary

- A **cyphertext** is the result of **encryption** performed on **plaintext** using an algorithm, called a **cipher**.

$$c = \text{encrypt}(m, k)$$

- **Decryption** is the reverse process.

$$m = \text{decrypt}(c, k)$$

Early encryption schemes [11]

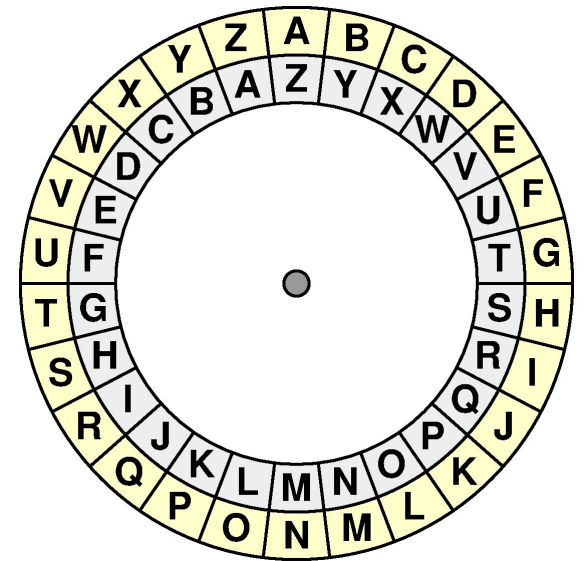
- 1500 BCE - clay tablets in Mesopotamia
 - Hides a recipe of pottery glaze
 - It used substitution as an encryption algorithm
 - The encryption was broken



[https://commons.wikimedia.org/wiki/
File:Tablet Rimush Louvre AO5476.jpg](https://commons.wikimedia.org/wiki/File:Tablet_Rimush_Louvre_AO5476.jpg)

Substitution

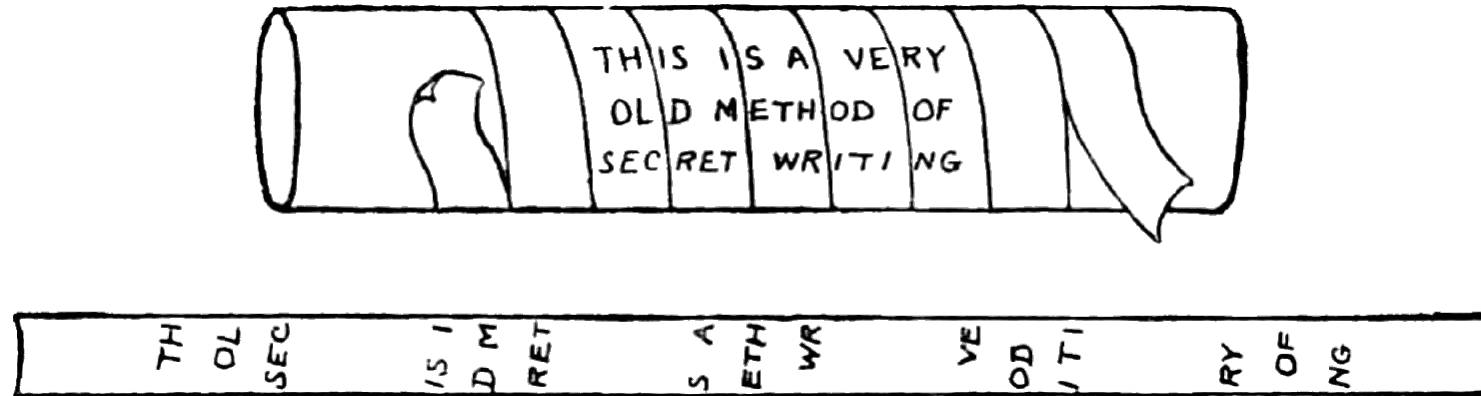
- Eg. Atbash system, used in the bible [12]
- Jeremiah 25:26: “And after all of them, the king of Sheshak will drink it too.” In original Hebrew, the word Sheshak commutes into “Babylon”.



<https://medium.com/@amangondaliya555/atbash-cipher-70e284ad921e>

Transposition

- The characters change their position in the text, but keep their original meaning
 - Eg. Encircles wood, called scytales, with paper (similar to Rail Fence Cipher [13])



<https://toebes.com/Flynns/Flynns-19241213.htm>

Fast forward on crypto history

- Caesar cipher (100 BCE – 44 BCE)
 - Shift cipher, e.g., $k=4 \Rightarrow A \rightarrow E, T \rightarrow X \dots$
 - Most of Caesar's enemies would have been illiterate \Rightarrow secure
- Vigenère cipher (1553 CE)
 - Poly-alphabetic substitution and transposition
- 1st & 2nd WW led to cipher machines, both for encryption (Enigma), decryption and for cracking (Bombe)



Modern cryptography

- What does an ideal cipher look like?
 - no correlation between plaintext, key and ciphertext
 - cannot recover key from known plaintext + ciphertext
 - Confusion & Diffusion!
- Do unbreakable algorithms exist?

The XOR operator

- Properties:

$$A \oplus B = B \oplus A$$

$$A \oplus 0 = A$$

$$A \oplus A = 0$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

$$(B \oplus A) \oplus A = B \oplus 0 = B$$

- Apply XOR between message & key, apply with key again to decrypt!

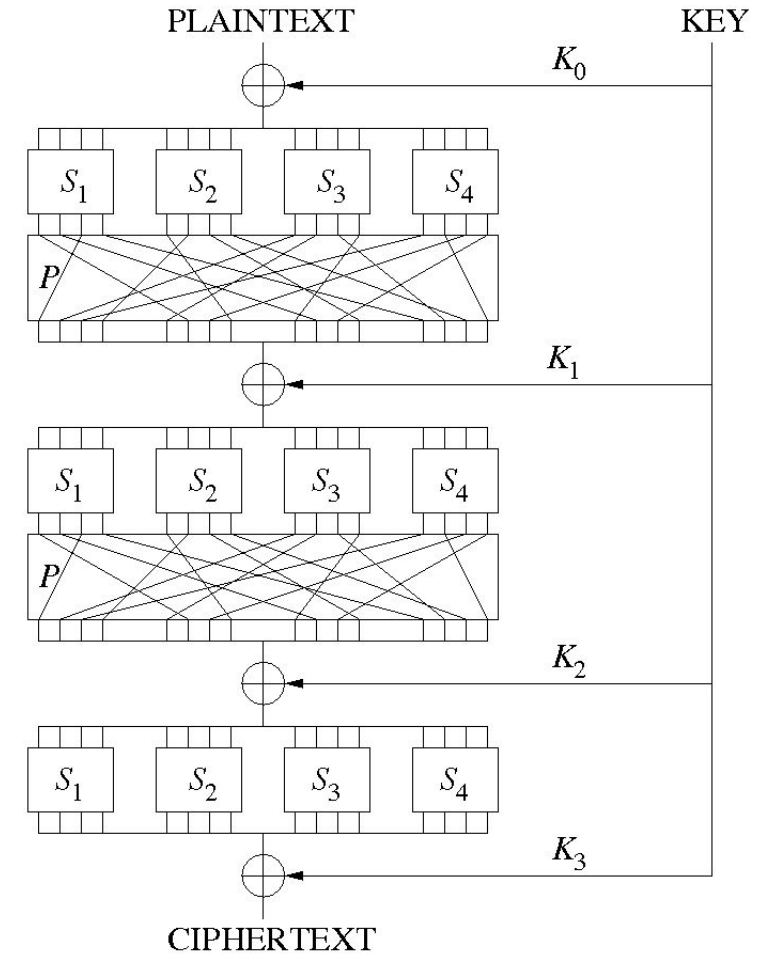
One-time Pad (Vernam, 1916)

- **One-time Pad** protects against **infinitely** powerful adversaries
 - XOR between a message and a same-length secret
 - **Bad news:** If you want to encrypt N bits of data, you need a N-bit secret key



Shannon's S-P network

- Claude Shannon - father of Information Theory (1949) [10]
- Substitution provides “confusion”
 - By building a complex binding between input and output
- Permutation (transposition) provides “diffusion”
 - By moving bits one single bit influences all output bits
- Encryption algorithms / functions MUST be invertible



From military to business



Encryption Schemes

- **Symmetric:**

- Same key used for both encryption and decryption
- Two variants: Block and Stream

- **Asymmetric:**

- Different keys: public <> private
- New feature: digital signatures!

Encryption Ideologies

- **Public Algorithms** – All the details of the algorithm are in the public domain, known to everyone.
 - Kerckhoffs' principle (Dutch cryptographer): *A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.*
 - Reformulated as Shannon's maxim: "the enemy knows the system", i.e., "*one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them*".
- **Proprietary algorithms** – The details of the algorithm are only known by the system designers and users.
 - security through obscurity.

Symmetric Ciphers

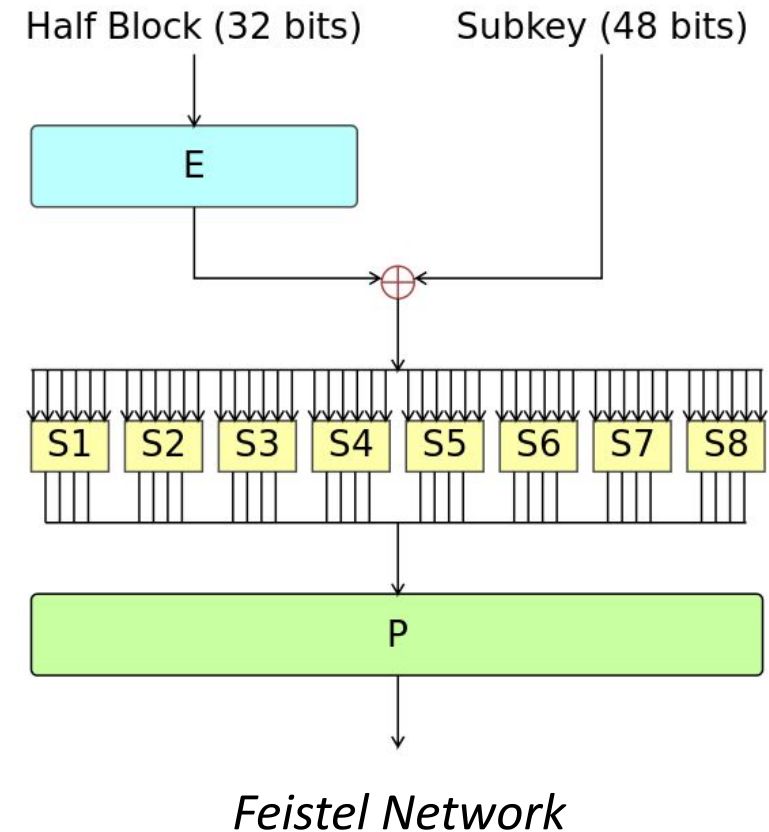
- A symmetric cipher is built of:
 - A “secret key” (data exchanged “in secret” by the two parties authorized to encrypt/decrypt)
 - An encryption algorithm
 - A decryption algorithm
- The strength of a cipher is given by:
 - Key size (small keys can be exhaustively search in a decent amount of time)
 - Algorithm strength (for example against statistical cryptanalysis)

Stream Ciphers

- **Keystream:** an “infinite” stream of bits generated from a key
- Operations (remember One Time Pad?):
 - $\text{keystream} \oplus \text{message} \Rightarrow \text{ciphertext}$
 - $\text{ciphertext} \oplus \text{keystream} \Rightarrow \text{original message}$
- The keystream must be **deterministic**, yet difficult to predict (without the original key)
- Popular algorithms: RC4 (deprecated / broken), Salsa20 / ChaCha (used by WireGuard)

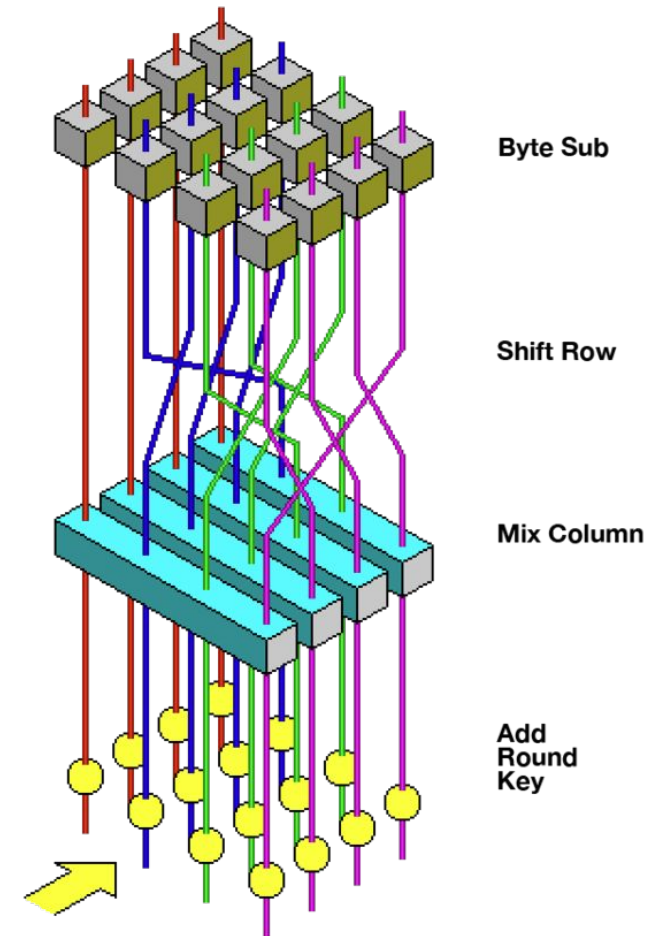
Block ciphers: DES (and 3DES)

- Developed by International Business Machines (IBM) as LUCIFER and modified by the National Security Agency (NSA).
 - LUCIFER used a key size of 128 bits however this was reduced to 56 bits for DES. 😊
- Adopted in 1977 as the Data Encryption Standard - DES
- Key length too small (56 bit) => brute force-able



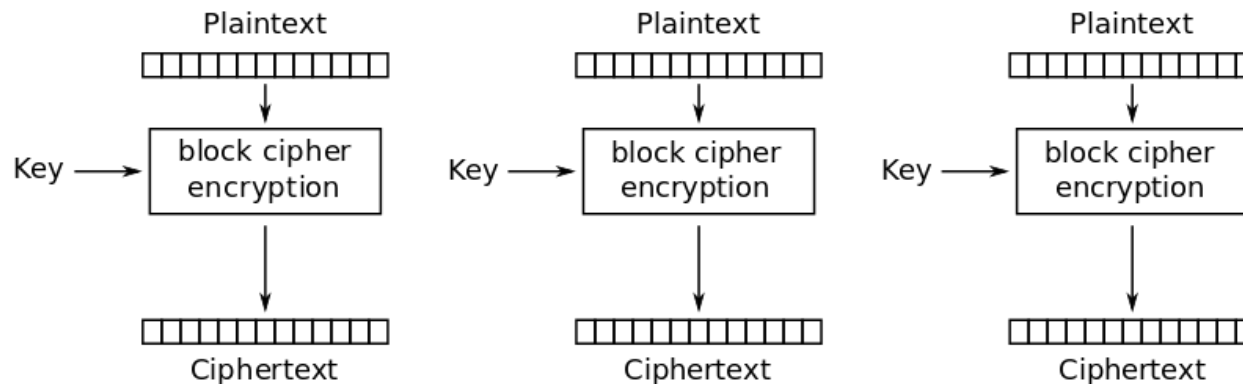
Block ciphers: AES

- In January 1997, NIST announced a competition for the successor to DES.
- NIST selected the winner, the Rijndael (pronounced "Rhine doll") algorithm of Belgian cryptographers Joan Daemen and Vincent Rijmen in October 2000.
- AES was approved for use with Secret and Top Secret classified information of the U.S. government in 2003.

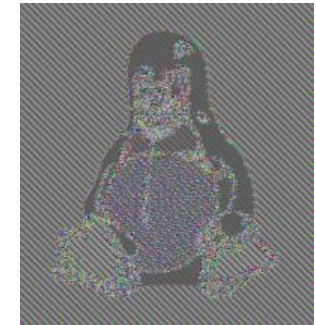


Block ciphers mode of operation (1)

- **Total Data Length >> Block Size!** (*e.g., 1MByte vs 128 bit*)
- **Electronic Codebook (ECB)**
 - Each block encrypted independently => identical plaintexts encrypted similarly
 - No chaining, no error propagation
 - **Does not hide data patterns**, unsuitable for long messages!



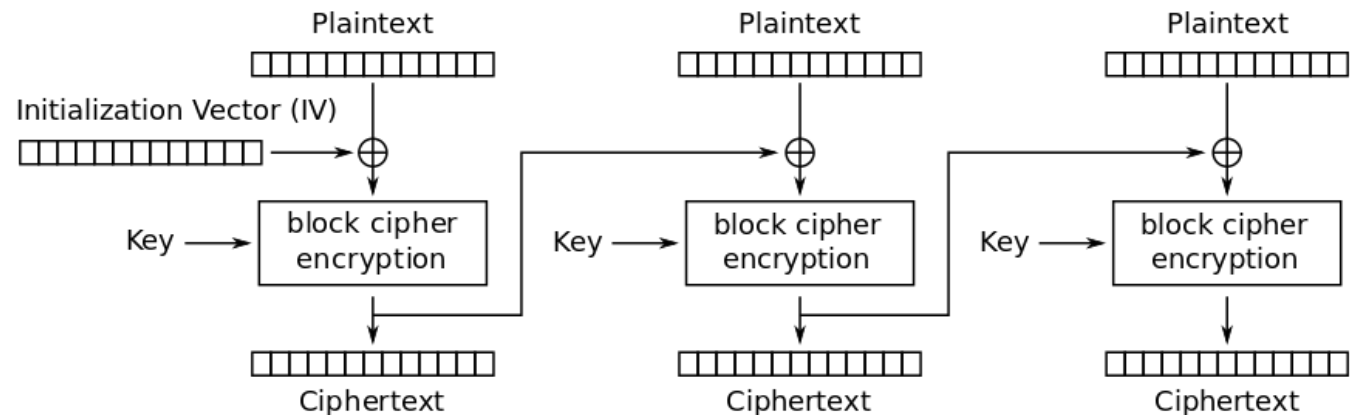
Electronic Codebook (ECB) mode encryption



Block ciphers mode of operation (2)

- **Cipher-Block Chaining (CBC)**

- Chaining: Ciphertext block c_j depends on x_j and all preceding plaintext blocks (dependency contained in c_{j-1})
- Identical messages result in different ciphertext, allows random access to ciphertext (decryption is still parallelizable)
- **Error propagation!**

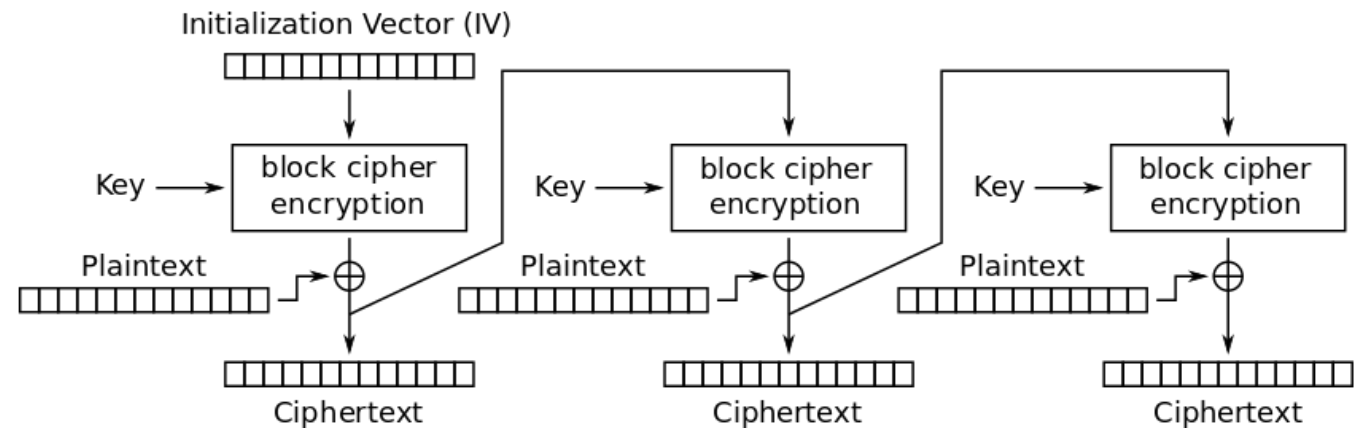


Cipher Block Chaining (CBC) mode encryption

Block ciphers mode of operation (3)

- **Cipher Feedback (CFB)**

- Random access to ciphertext
- Decryption is parallelizable
- Identical messages: as in CBC
- Chaining: Similar to CBC
- Error propagation...

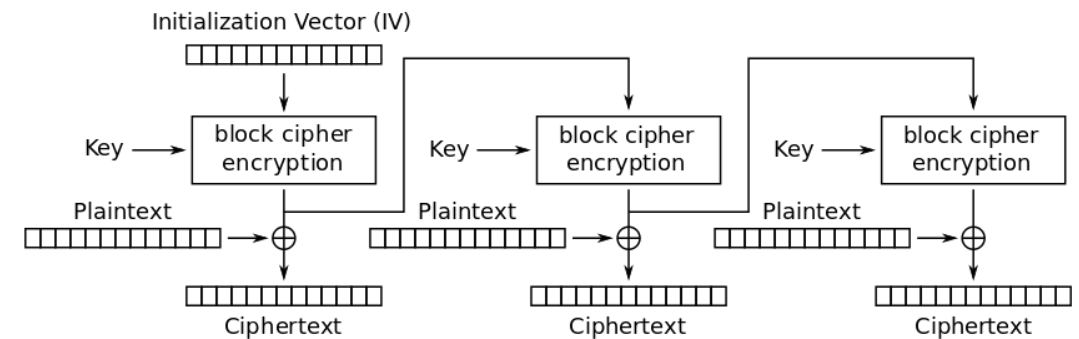


Cipher Feedback (CFB) mode encryption

Block ciphers mode of operation (4)

- **Output Feedback (OFB)**

- Preprocessing possible (keep enc/decrypting previous output block)
- No random access, not parallelizable
- Identical messages: same as CBC
- No chaining dependencies
- Error propagation: Single bit error on c_j may only affect the corresponding bit of x_j
- IVs should not be reused!

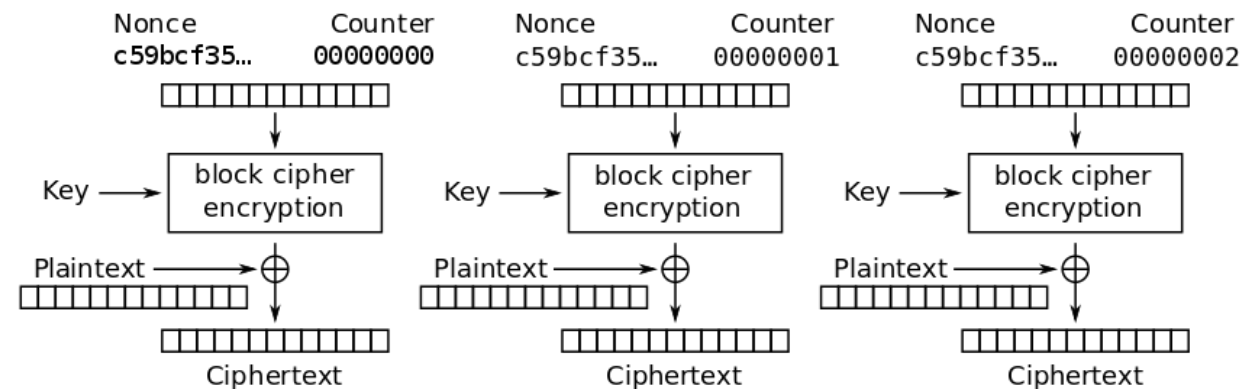


Output Feedback (OFB) mode encryption

Block ciphers mode of operation (5)

- **Counter (CTR) / GCM**

- Preprocessing possible
- Allows random access
- Both encryption & decryption are parallelizable
- Identical messages: changing nonce results in different ciphertext
- No chaining dependencies
- No error propagation
- Nonce should be random, and should be changed if a previously used key is to be used again



Counter (CTR) mode encryption

Which Mode for What Task?

- General file or packet encryption: CBC.
 - Input must be padded to multiple of cipher block size
- Resiliency / loss of ciphertext: CFB
- Noisy line / no error propagation: OFB
- High-speed data processing: CTR / GCM
- *Integrity check is required*

Problem description

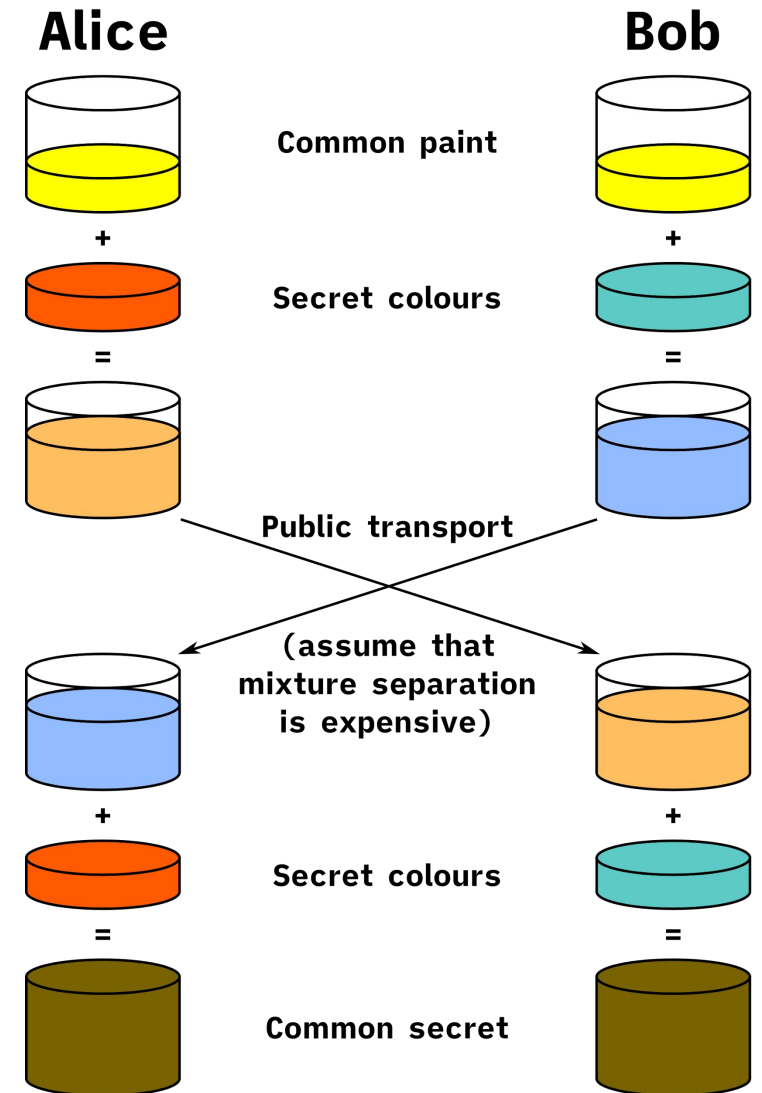
- Symmetric key distribution... how to do securely?
- Can two parties agree on a shared secret without private communication? [Ralph Merkle]
 - (April 1975). "Secure Communications Over Insecure Channel"

Diffie - Hellman (1976)

- One of the earliest public-key protocol
- Took Merkle's idea and improves it such that the attacker requires exponential computations
- Establish a secret between 2 (possibly unacquainted) parties!
- Security: discrete logarithm problem (NP-complete)

Diffie - Hellman

- **Common paint:**
 p = public modulus (prime), $p = 5$
 g = public generator/base (primitive root), $g = 2$
 a = Alice's private key, $a = 4$
 b = Bob's private key, $b = 6$
- **Public exchanges:**
Alice's public key -> Bob:
 $A = g^a \pmod p = 2^4 \pmod 5 = 1$
Bob's public key -> Alice:
 $B = g^b \pmod p = 2^6 \pmod 5 = 4$
- Alice computes secret/key:
 $s = B^a \pmod p = 4^4 \pmod 5 = 1$
- Bob computes secret:
 $s = A^b \pmod p = 1^6 \pmod 5 = 1$



RSA (1977)

- Ron Rivest, Adi Shamir, and Leonard Adleman
- Key pair:
 - Private key: p, q => decryption key
 - Public key: $n = p * q, e$
- Security: factorization problem!
- Primitives:
 - $c = \text{encrypt}(m, \text{PubKey})$
 $m = \text{decrypt}(c, \text{PrivKey});$
 - $s = \text{sign}(m, \text{PrivKey})$
if ($\text{verify}(s, \text{PubKey})$) ...

$$c \equiv m^e \pmod{n}.$$

$$c^d \equiv (m^e)^d \equiv m \pmod{n}.$$

The UK version

- James H. Ellis came up with the idea of non-secret encryption in 1970 (5 years before Merkle)
- Clifford Cocks invented equivalent of RSA in 1973 (3-years before RSA)
- Malcolm J. Williamson invented the equivalent of DH in 1974 (2-years before DH)
- ...
- *[yep, no profit!]*
- Government Communications Headquarters (GCHQ) decided to keep the discoveries secret till 1998.

Elliptic Curve Cryptography

- Another approach to asymmetric encryption
- Elliptic curves in finite fields instead of finite Galois fields:

$$y^2 = x^3 + ax + b$$

- Smaller numbers for equivalent security (e.g., 384 vs 4096 bits)
- Same domain parameters (e.g., p , a , b , G , n , h)
=> standard curves (e.g., NIST)!
- Algorithms:
 - ECDH
 - ECIES
 - ECDSA
 - EdDSA etc.

Message digest functions (hashing)

- One-way functions that provides data “summarization”
 - Message integrity, key derivation
- Collisions exist but should be hard to find
- Popular algorithms:
 - MD5 (broken): 1991, 128 bits
 - SHA-1 family (1995): 160 bits
 - SHA-2 family (2001), SHA-3 (2010): 256-512 bits

Practical Integrity

- Hashing is not enough because an attacker can simply change the message and the Hash value
- MAC (message authentication code) uses a secret key together with the function
 - HMAC – function is hashing
 - CBC-MAC (function is CBC encryption mode)
- Asymmetric signature: RSA, DSA, ECDSA etc.

Attacks On Cryptosystems

Passive Attacks

- No communication with victim
- Stealing of private data without the know of the victim

Active Attacks

- Involves changing data with victim
- Unauthorized data access in order to modify/delete/alter it

Types of attacks

- **Ciphertext Only Attacks (COA)** – The attacker has access to a set of ciphertext(s), and not to the corresponding plaintext. Successful when the corresponding plaintext can be determined from a given set of ciphertext.
- **Known Plaintext Attack (KPA)** – The attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. Typically, this may be done by determining the key.
- **Chosen Plaintext Attack (CPA)** – The attacker has the text of his choice encrypted. This simplifies his task of determining the encryption key.
- **A chosen-ciphertext attack (CCA)** – The attacker can gather information by obtaining the decryptions of chosen ciphertexts. The adversary can attempt to recover the key used for decryption.

Types of attacks

- **Dictionary Attack** – The attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.
- **Brute Force Attack (BFA)** – In this method, the attacker tries to determine the key by attempting all possible keys.
- **Man in Middle Attack (MIM)** – The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
- **Side Channel Attack (SCA)** – This type of attack is launched to exploit the weakness in physical implementation of the cryptosystem.
- **Timing/Power Analysis Attacks** – They exploit the fact that different computations take different times to compute on processor.

Practicality of Attacks

- Highly academic
 - Weaker versions, e.g., AES with fewer rounds
- Unrealistic assumptions
 - In chosen-ciphertext attack, the attacker requires an impractical number of deliberately chosen plaintext-ciphertext pairs.

Post-quantum cryptography

- Equation 1 shows the time it takes to run the fastest known algorithm (GNFS) to compute a prime factorization on a binary formatted processor. Equation 2 shows the algorithm discovered by Peter Shor that computes a prime factorization on a quantum computer. In both cases, "b" is the number of bits in the number.

$$e^{\left[\left(\frac{64}{9} * b\right)^{\frac{1}{3}} (\log b)^{\frac{2}{3}}\right]}$$

Equation 1. GNFS algorithm time.

$$b^3$$

Equation 2. Shor's algorithm time.

Homomorphic encryption

- Allows computations on encrypted data
- Not many operations are supported
 - Mostly addition and multiplication
- In 2020 there was a solution for encrypted machine learning

Resources

[1] https://en.wikipedia.org/wiki/History_of_cryptography

[2] https://www.tutorialspoint.com/cryptography/attacks_on_cryptosystems.htm

[3] https://en.wikipedia.org/wiki/Caesar_cipher

[4] http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/des%20history.html

[5] http://www.utdallas.edu/~muratk/courses/crypto07_files/modes.pdf

Resources

[6] <http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html>

[7]

<https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730>

[8]

<http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf>

[9] “Indistinguishability Obfuscation from Well-Founded Assumptions”,
Aayush Jain and Huijia Lin and Amit Sahai

Resources

[10] (“Communication Theory of Secrecy Systems”, By C. E. SHANNON)
<https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf>

[11]
<https://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/> (on 03.11.2022)

[12] <https://www.gotquestions.org/Atbash-code.html> (on 03.11.2022)

[13]
[http://cochranmath.pbworks.com/w/page/118045167/Transposition%20Ciphers#:~:text=will%20be%20discussed\).-,History,Civil%20War%20used%20route%20ciphers](http://cochranmath.pbworks.com/w/page/118045167/Transposition%20Ciphers#:~:text=will%20be%20discussed).-,History,Civil%20War%20used%20route%20ciphers) (on 03.11.2022)