Basics of Cryptography

Chapter 1

Vigenère Cipher

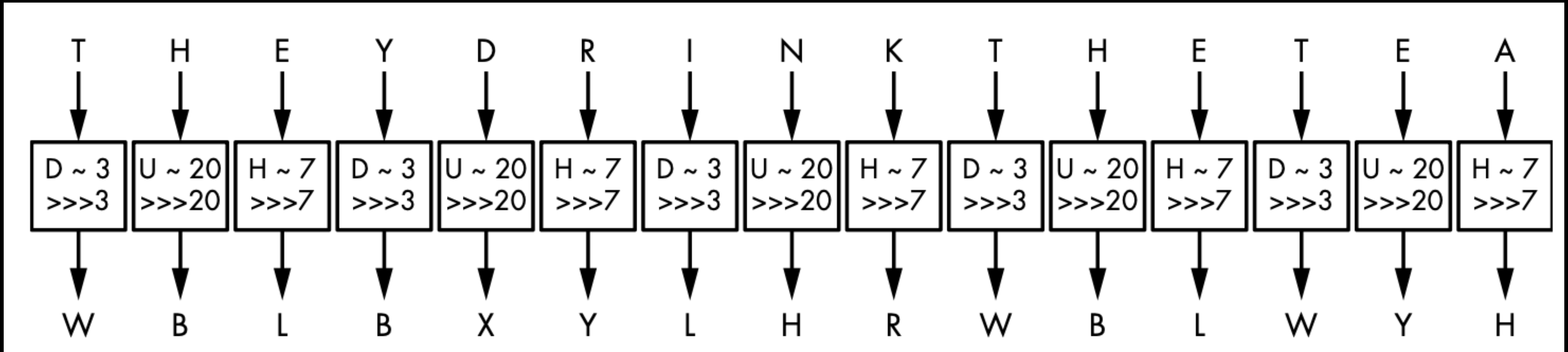
- Similar to the Caesar cipher, except that letters are shifted by values defined by a key.
  - The key is a collection of letters that represent numbers based on their position in the alphabet.

- For example, if the key is DUH, letters in the plaintext are shifted using the values D=3, U=20, H=7.

- The 3, 20, 7 pattern repeats until you’ve encrypted the entire plaintext.

Vigenère Cipher

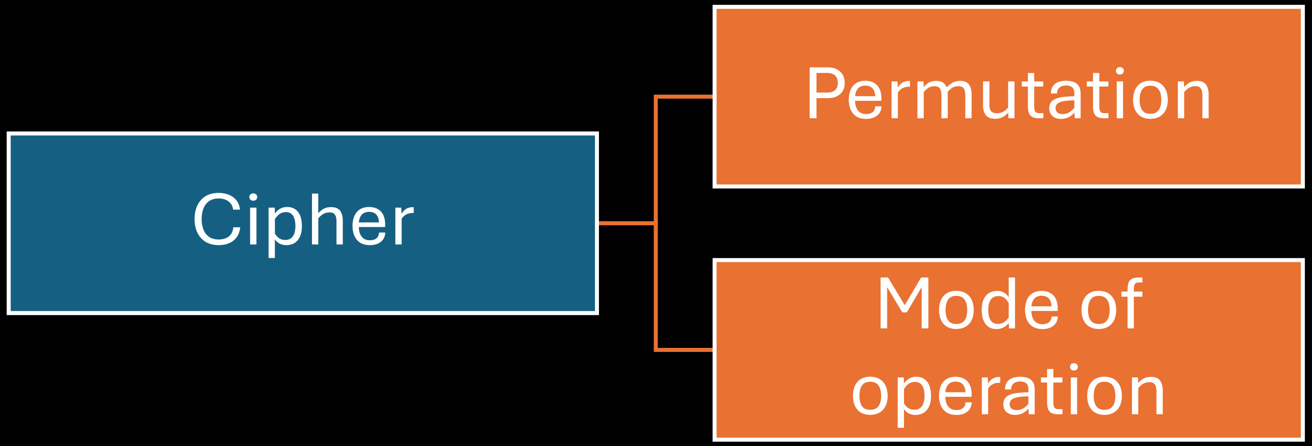
- Example: encrypting the sentence THEY DRINK THE TEA using the keyword DUH



Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

How Ciphers Work?

- Each cipher has two components:

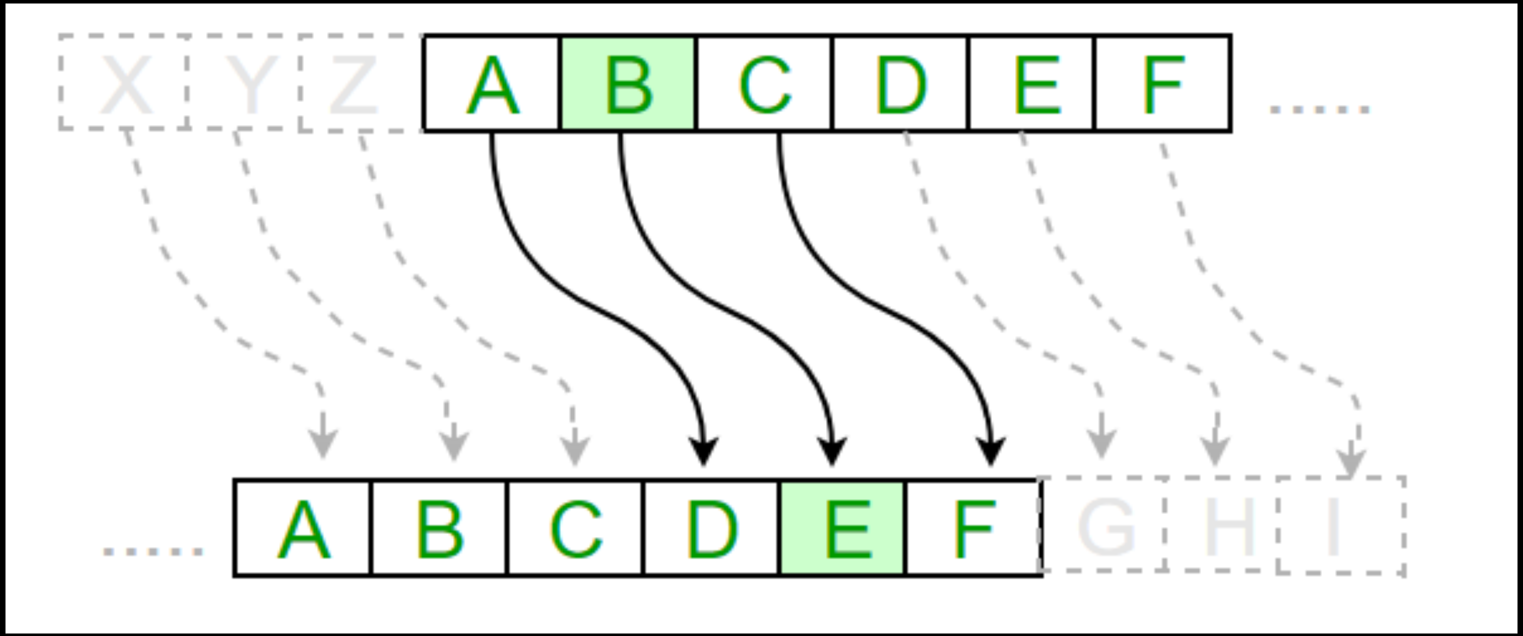


A function that transforms an item (a letter or a group of bits) such that each item has a unique inverse.

An algorithm that uses a permutation to process messages of arbitrary size.

How Ciphers Work?

- In Caeser cipher:
  - **Permutation**: just shifting the letters.
  - **Mode of operation**: repeating the same permutation, shifting, for each letter.



How Ciphers Work?

- Vigenère cipher has a more complex mode:
  - **Permutation**: as Caeser cipher, just shifting each letter.
  - **Mode of operation**: shifting is different for each letter.

Plain Text	P	A	S	S	W	O	R	D
Key	K	E	Y	K	E	Y	K	E
Cipher Text	Z	E	Q	C	A	M	B	H

Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

The Permutation

- Most of the classical ciphers replace each letter with another letter.
  - They are performing *substitution* – shifting in the alphabet.
- A “substitution” is different from a “permutation”.
- For example:
  - A function that transforms A, B, C, D to G, K, A, Y is a “substitution”
  - A function that transforms A, B, C, D to C, A, D, B is a “permutation”

The Permutation

- Not every permutation is secure.
- A secure permutation satisfies three criteria:

The permutation should be determined by the key.

Different keys should result in different permutations.

The permutation should look random.

Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Mode of Operation

- Given a secure permutation that transforms A to X, B to M, and N to L.
- Then, to encrypt BANANA, we get MXLXLX.
- Same permutation → reveals duplicate letters → insecure.
- Analyzing these duplicates → learn something about the message.

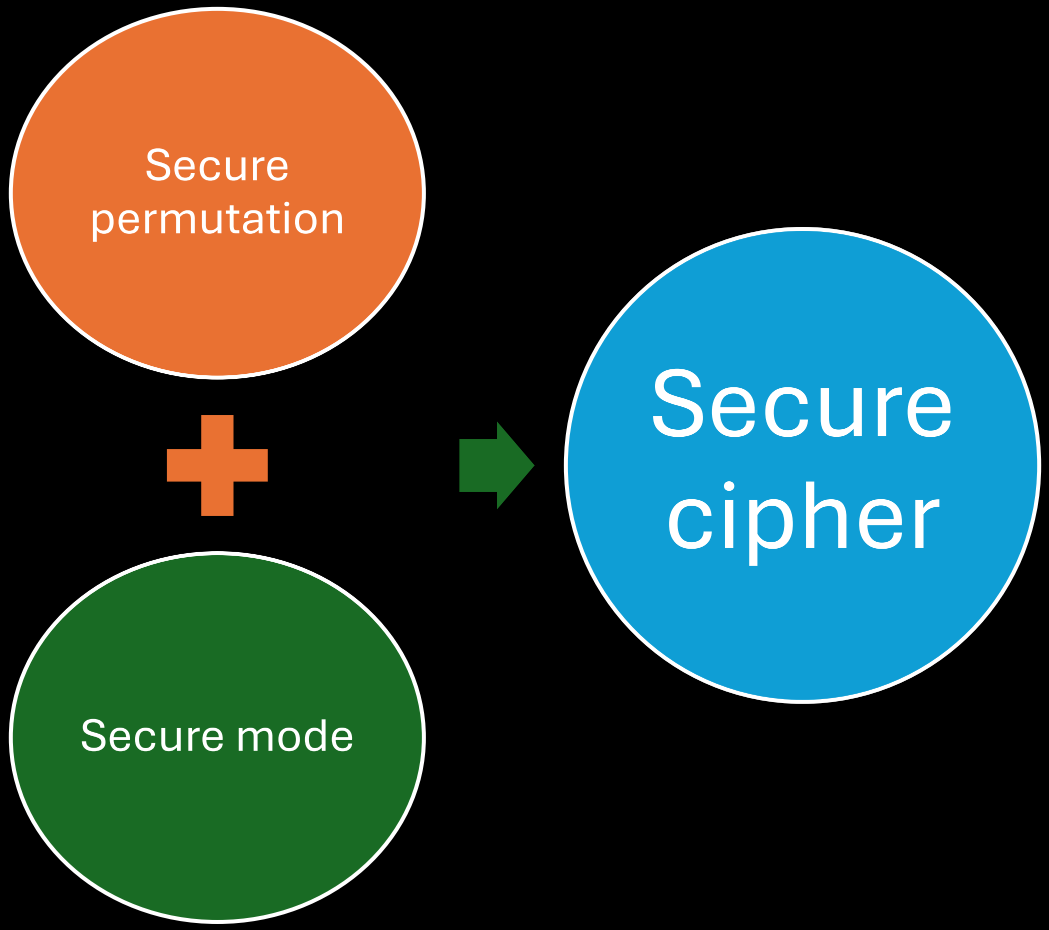
Mode of Operation

- The mode of a cipher mitigates the exposure of duplicate letters in the plaintext by using different permutations for duplicate letters.

- Vigenère cipher: if the key is N letters, then N different permutations will be used for every N consecutive letters.
  - This can still result in patterns in the ciphertext because every Nth letter of the message uses the same permutation.

- Frequency analysis can be used to break Vigenère cipher.

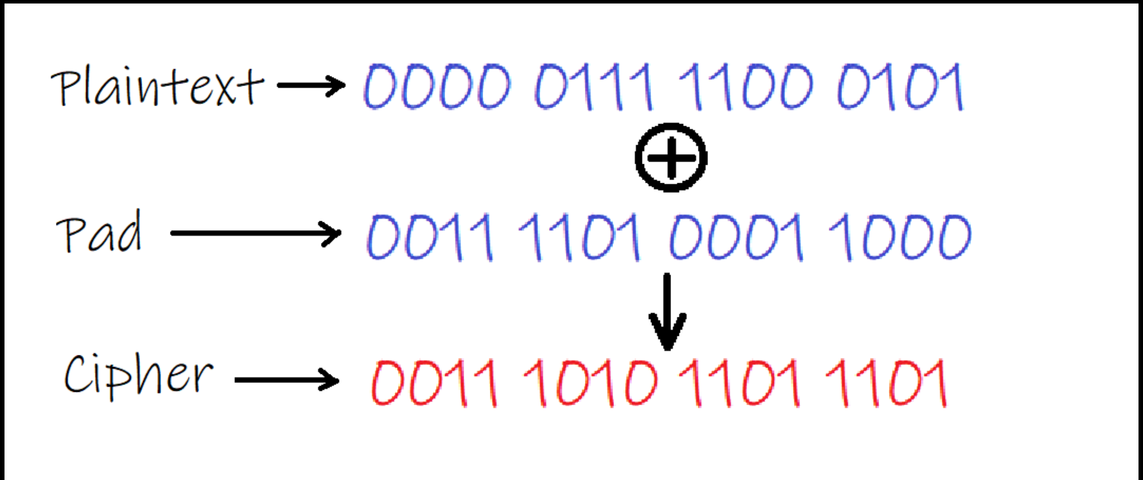
The Mode of Operation



Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

The One-Time Pad

- OTP uses a **single-use** key that is larger ≥ the size of the plaintext.



- **Perfect secrecy**: if an attacker has unlimited computing power, it’s impossible to learn anything about the plaintext, but its length.

The One-Time Pad

Example: P = 01101101 and K = 10110100, then

- To encrypt: $C = P \oplus K = 01101101 \oplus 10110100 = 11011001$
- To decrypt: $P = C \oplus K = 11011001 \oplus 10110100 = 01101101$

	P	0	1	1	0	1	1	0	1
Encrypt: XOR	K	1	0	1	1	0	1	0	0
	C	1	1	0	1	1	0	0	1
Decrypt: XOR	K	1	0	1	1	0	1	0	0
	P	0	1	1	0	1	1	0	1

The One-Time Pad

- Each key K MUST be used only once.
  - If the same K is used to encrypt P_1 and P_2 to C_1 and C_2, then an eavesdropper can compute the following:

$$C_1 \oplus C_2 = (P_1 \oplus K) \oplus (P_2 \oplus K) = P_1 \oplus P_2$$

- Thus, an eavesdropper can learn the XOR difference of P_1 and P_2.
  - If either plaintext message is known, then the other message can be recovered.

- OTP is inconvenient: to encrypt a one-terabyte hard drive, you'd need another one-terabyte drive to store the key!

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Encryption Security

- Two concepts describe the security of a cipher:
  - **Attack models**: assumption about what an attacker can do.
  - **Security goals**: description of what is considered a successful attack.

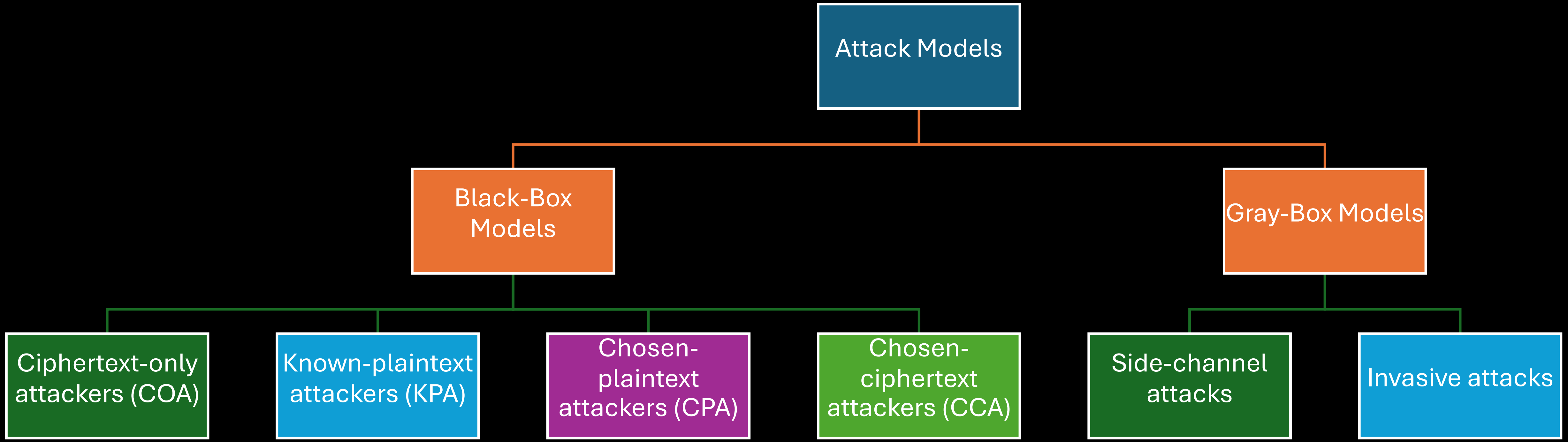
- Security notion = Attack model + Security goal:
  - We say: a cipher achieves <u>a certain security notion</u> if any attacker working in a <u>given model</u> can't achieve the <u>security goal</u>.

Encryption Security: Attack Models

- **Attack model**: a set of assumptions about how attackers interact with a cipher and what they can and can’t do.

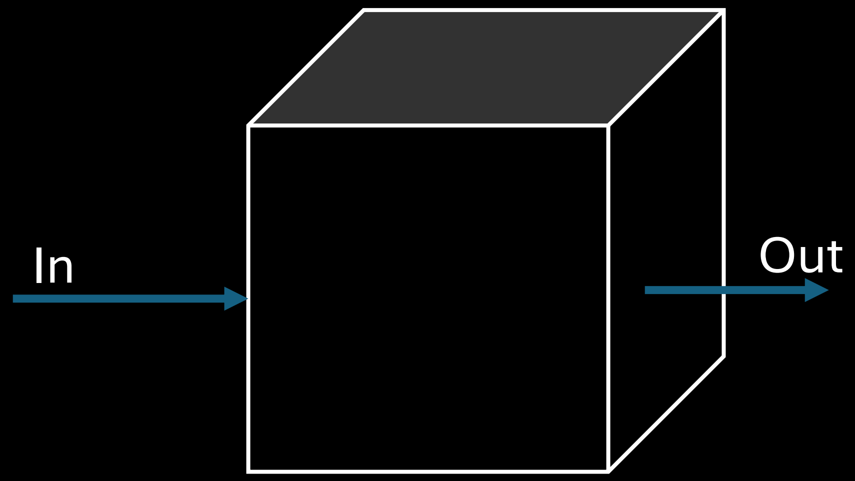
- Kerkhoff's Principle:
  - The encryption algorithm is known.
  - The security of a cipher relies on the <u>**key**</u> and the mechanism of the cipher.

Encryption Security: Attack Models

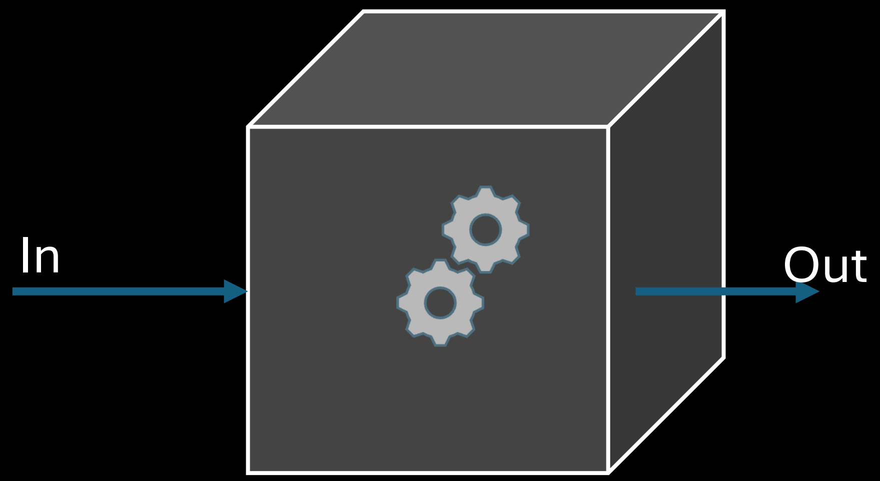


Encryption Security: Attack Models

- Black box models: attackers can see the input/output of a cipher only.
- Gray box models: attackers have access to a cipher’s implementation.



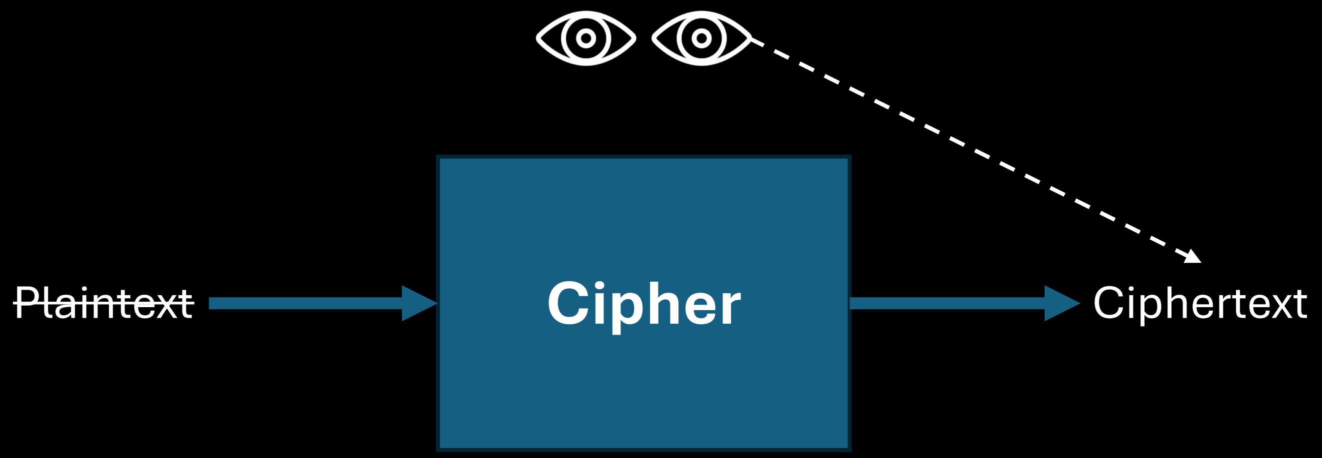
No knowledge



Some knowledge

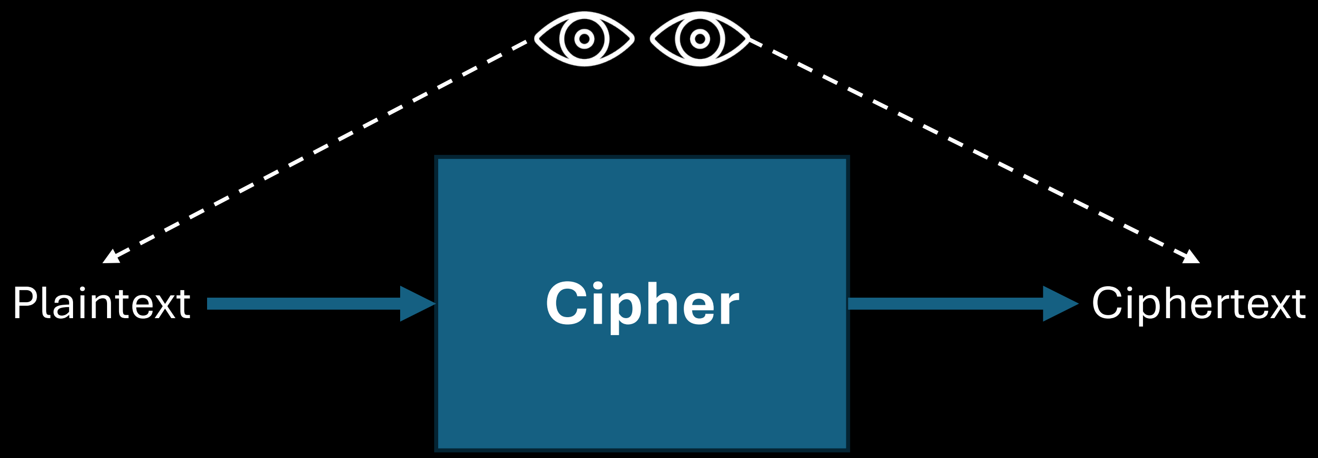
Encryption Security: Attack Models

1. **Ciphertext-only attackers (COA)** observe ciphertexts but don't know the associated plaintexts.
   - Attackers in the COA model are passive and can't perform encryption or decryption queries.



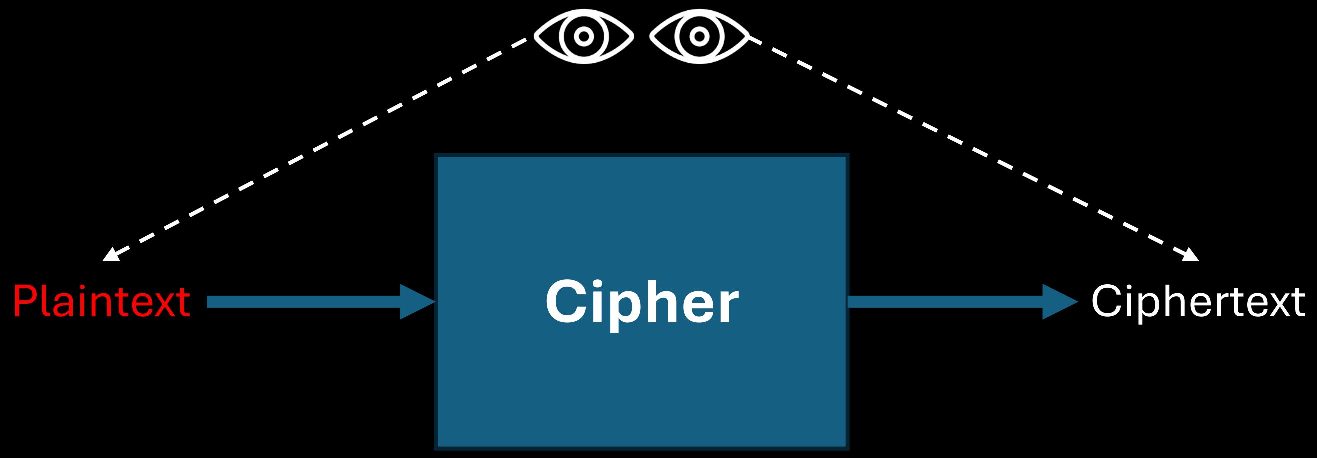
Encryption Security: Attack Models

2. **Known-plaintext attackers (KPA)** observe ciphertexts and know the associated plaintexts.
    - Attackers in the KPA model thus get a list of plaintext–ciphertext pairs,
    - KPA is a passive attacker model.



Encryption Security: Attack Models

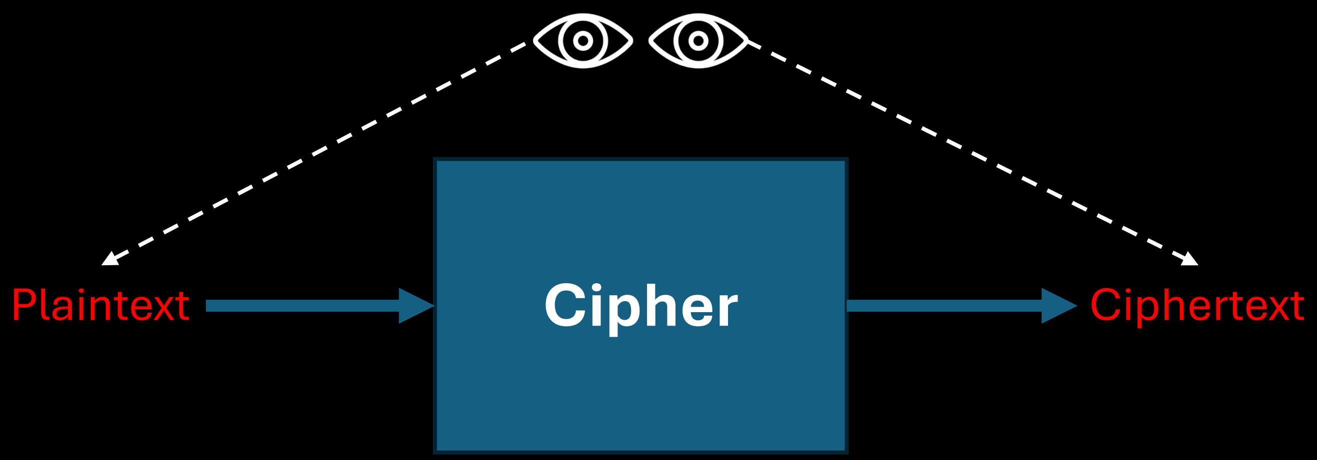
3. **Chosen-plaintext attackers (CPA)** can perform encryption queries for plaintexts of their choice and observe the resulting ciphertexts.
   - Attackers choose all or part of the plaintexts and then observe the ciphertexts.
   - CPA are active attackers, because they influence the encryption processes rather than passively eavesdropping.



Encryption Security: Attack Models

4. **Chosen-ciphertext attackers (CCA)** can both encrypt and decrypt; perform encryption queries and decryption queries.

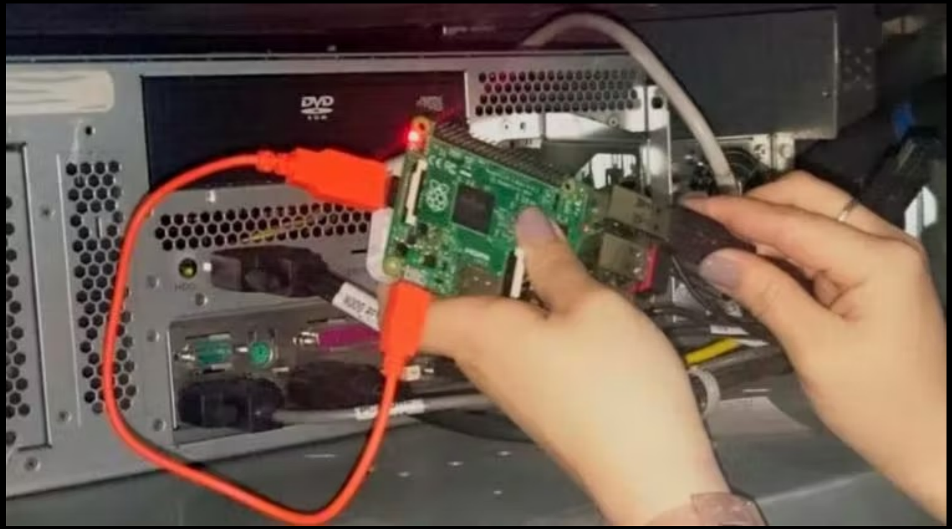
- CCA are active attackers



Encryption Security: Attack Models

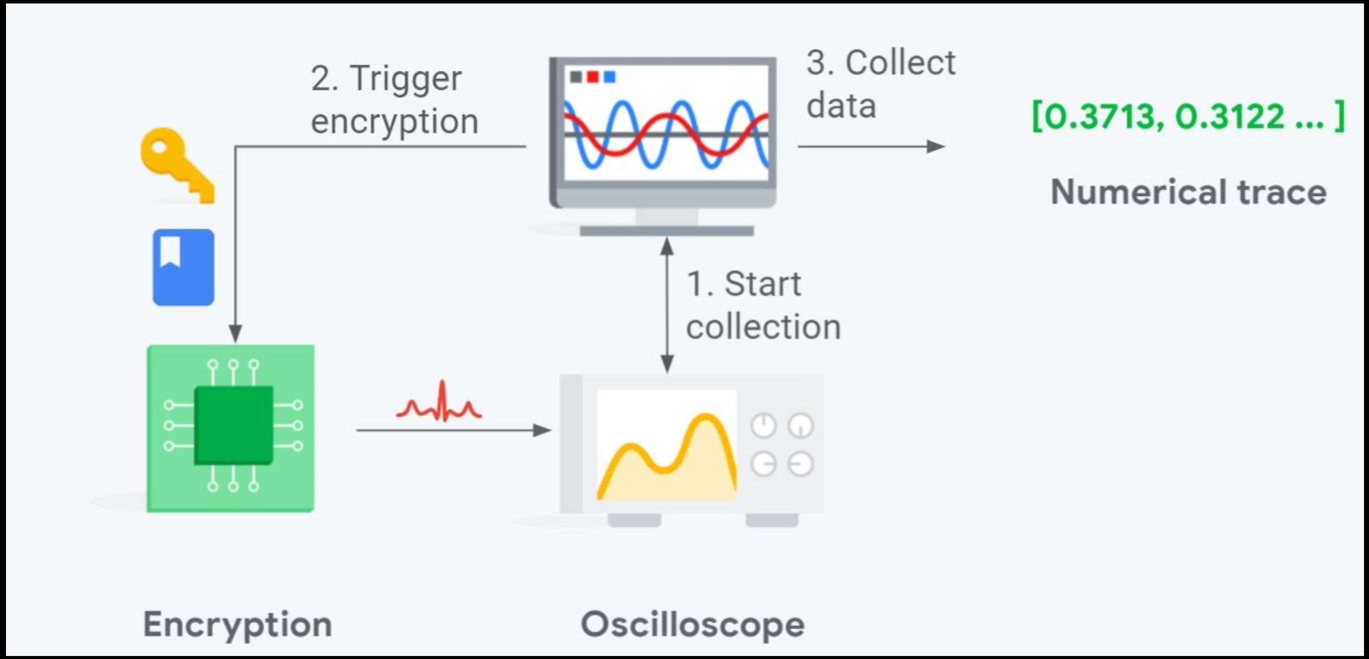
- Gray box models: attackers have access to a cipher’s implementation.
  - More realistic for applications such as smart cards, embedded systems.
  - Attackers have physical access and can tamper with the algorithms’ internals.

Check CSAW-ESC



Encryption Security: Attack Models

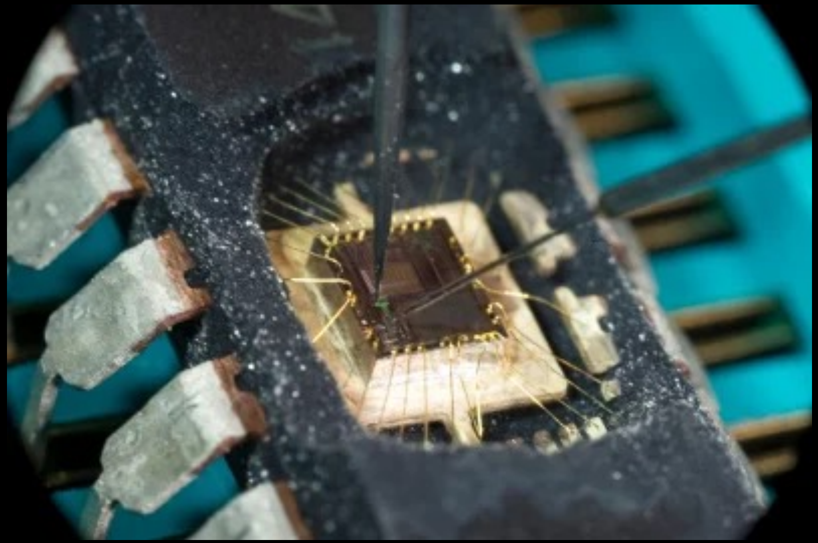
- Gray box models:
  1. **Side-channel attacks**: an attacker exploits the leakage of physical information from a system during the execution of an application.
     - They are noninvasive.

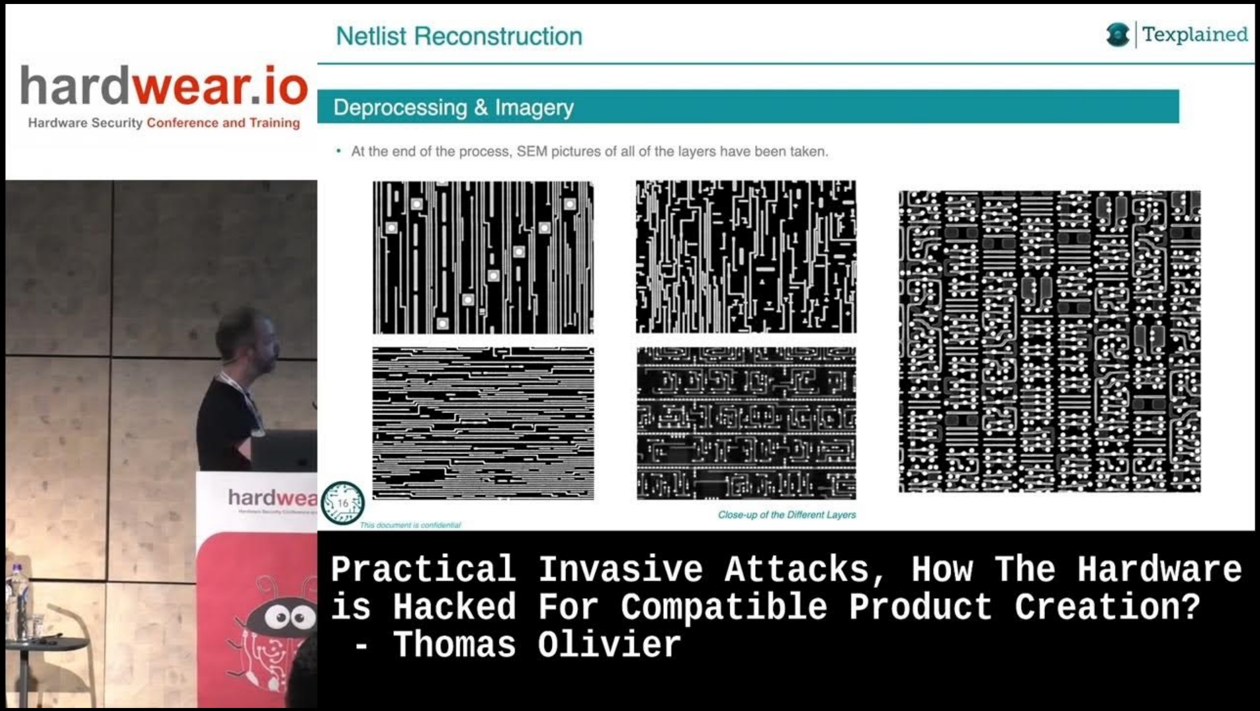


Encryption Security: Attack Models

- Gray box models:

  2. **Invasive attacks**: require direct access to the internal components of the device, which requires a well-equipped and knowledgeable attacker to succeed.
     - Require tools such as a high-resolution microscopes and a chemical lab.





Encryption Security: Security Goal

- Security goal: nothing can be learned about the cipher's behavior.
- Two main security goals:
  1. **Indistinguishability (IND).** Ciphertexts should be indistinguishable from random strings.

  2. **Non-malleability (NM).** Given a ciphertext $C_1 = E(K, P_1)$, it's impossible to create another ciphertext, C_2, whose corresponding plaintext, P_2, is related to P_1 in a meaningful way.
     - The OTP is malleable: given a ciphertext $C_1 = P_1 \oplus K$, you can define $C_2 = C_1 \oplus 1$, which is a valid ciphertext of $P_2 = P_1 \oplus 1$ under the same key K.

Encryption Security: Security Notion

- Security goals are only useful when combined with an attack model.

- The convention is to write a security notion as GOAL-MODEL.
    - IND-CPA
    - IND-CCA
    - NM-CPA
    - NM-CCA

Encryption Security: Security Notion

- The most important one: semantic security – IND-CPA.
- IND-CPA = ciphertexts don't leak any information about plaintexts as long as the key is secret.
- To achieve IND-CPA security, encryption must return different ciphertexts if called twice on the same plaintext.
  - This is can be achieved using **randomized encryption**.

Encryption Security: Security Notion

- In IND-CPA, encryption is expressed as $C = E(K, R, P)$
  - C is the result ciphertext
  - E is the encryption function
  - R is fresh random bits
  - K is the secret key
  - P is the plaintext

- Decryption is expressed as $P = D(K, R, C)$

Encryption Security: Security Notion

- To construct a semantically secure cipher, use a deterministic random bit generator (DRBG).

- **DRBG**: an algorithm that returns random looking bits given some secret value.
- Encryption becomes:

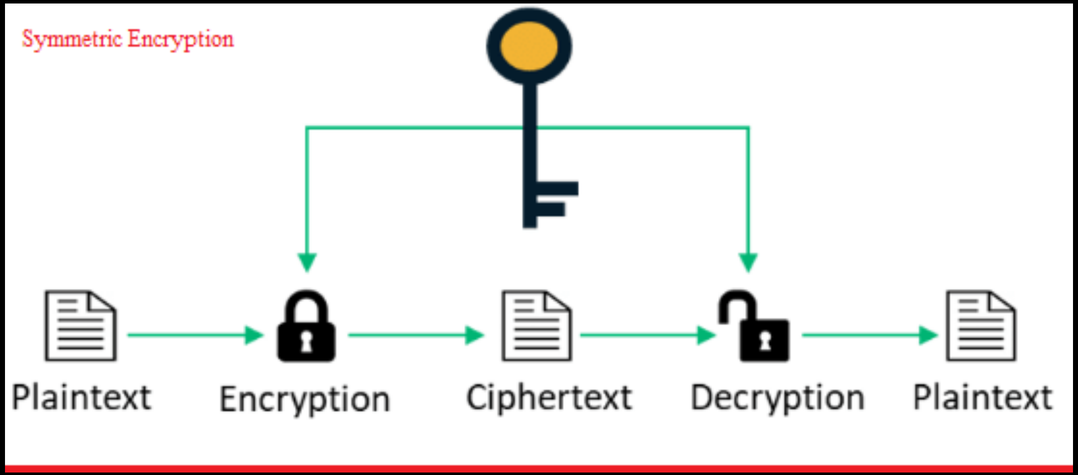
$$E(K, R, P) = (DRBG(K||R) \oplus P, R)$$

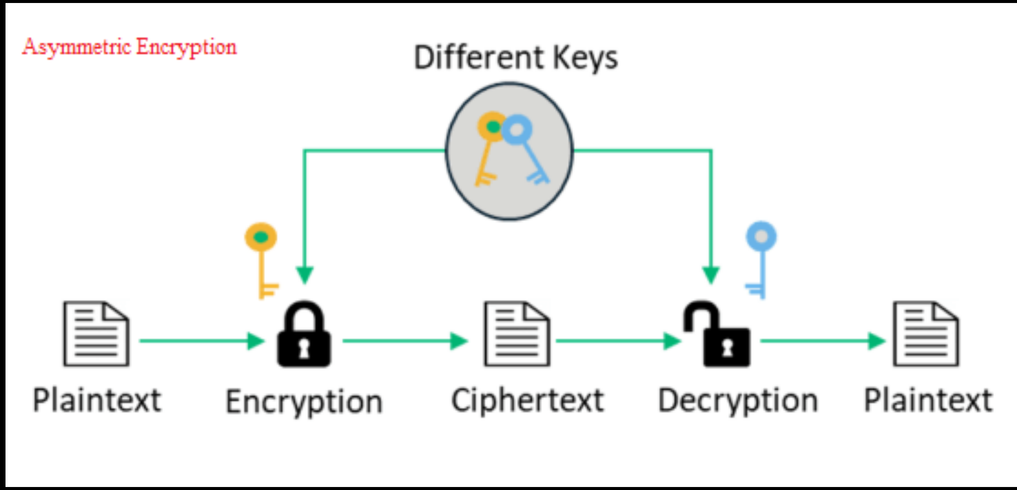
  - $K||R$ means concatenating the key with random bits.

Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Asymmetric Encryption

- Symmetric encryption: use one key for encryption and decryption.
- In asymmetric encryption, there are two keys:
  - The **encryption** key (**public key**),publicly available to anyone who wants to send you encrypted messages.
  - The **decryption** key must remain secret and is called a **private** key.



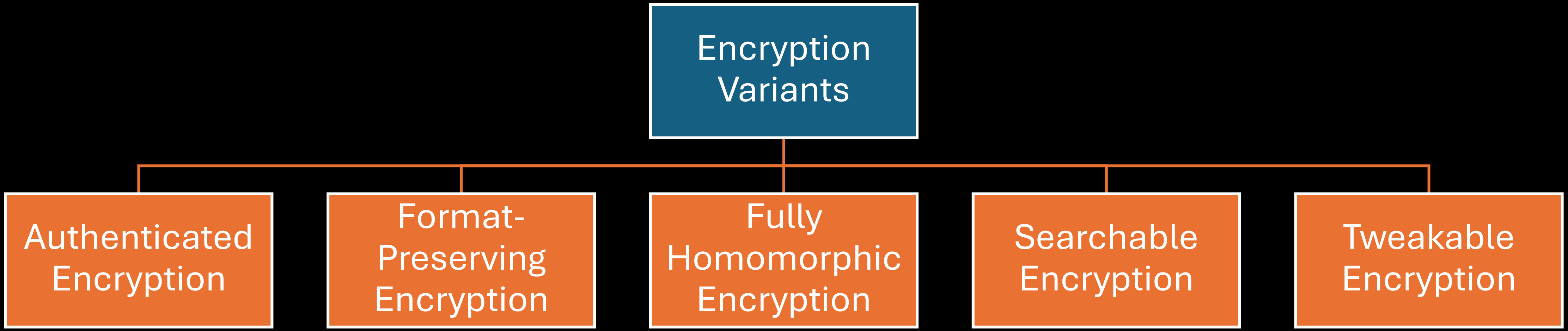


Asymmetric Encryption

- The public key can be computed from the private key.
- The private key can’t be computed from the public key.

Content
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

When Ciphers Do More Than Encryption



When Ciphers Do More Than Encryption

Authenticated Encryption:

- A symmetric encryption that returns an authentication tag and a ciphertext.
- $AE(K, P) = (C, T)$
  - The tag T is a short string that's impossible to guess without the key.
- The tag ensures the integrity of the message.
  - Evidence that the ciphertext received is identical to the one sent in the first
- Decryption takes K, C, and T and returns P only if it verifies that T is valid otherwise, it aborts and returns some error.

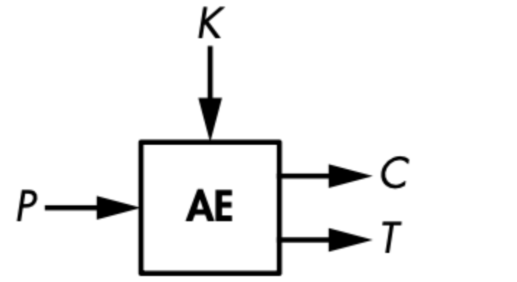


Figure 1-4: Authenticated encryption

When Ciphers Do More Than Encryption

Authenticated encryption with associated data (AEAD):

- An extension of authenticated encryption that takes some cleartext and unencrypted data and uses it to generate the authentication tag.

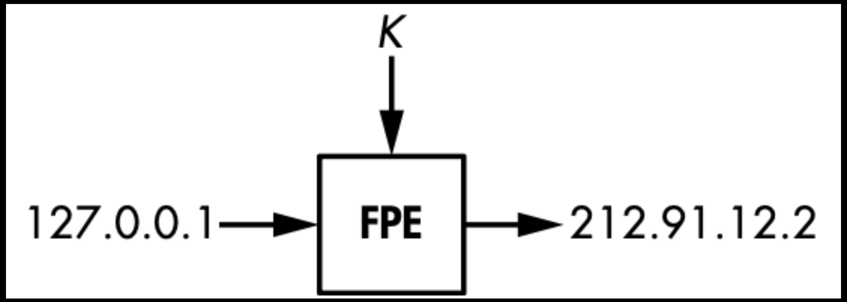
- AEAD(K, P, A) = (C, T).

- Can be used to protect protocols' datagrams with a cleartext header and an encrypted payload.
  - Destination addresses need to be clear in order to route network packets.

When Ciphers Do More Than Encryption

Format-Preserving Encryption:

- It can create ciphertexts that have the same format as the plaintext.
- For example, FPE can encrypt
  - IP addresses to IP addresses
  - ZIP codes to ZIP codes,
  - credit card numbers to credit card numbers



When Ciphers Do More Than Encryption

Fully Homomorphic Encryption:

- Enables computing a function on a ciphertext without the need to decrypting it.
- In FHE:
  - If we need to compute a function F on a plaintext P to get a result.
  - FHE encrypts P to C and transforms F to F`.
  - Then compute F`(C) to C`.
  - When decrypting C`, we get F(P).
- Downside: very slow.

When Ciphers Do More Than Encryption

Searchable Encryption:

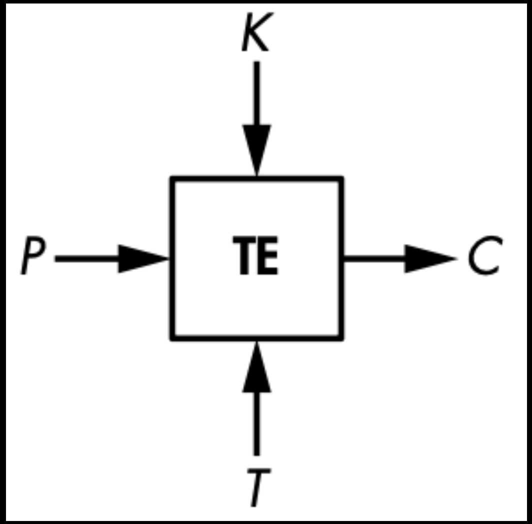
- Enables searching over an encrypted database without leaking the searched terms by encrypting the search query itself.

- FHE and searchable encryption enhance the privacy of cloud-based applications by hiding your searches from your cloud provider.

When Ciphers Do More Than Encryption

Tweakable Encryption:

- Similar to basic encryption, except it has a parameter called a *tweak*.
  - aims to simulate different versions of a cipher.



- The main application is disk encryption.
  - It uses a tweak value that depends on the position of the data encrypted, which is usually a sector number or a block index.

TASK

- Implement the Vigenère cipher. Encrypt the message “I LOVE CRYPTO” using the key “BAD”
- Implement the OTP cipher. Use $secret$ module in Python to generate a secure random key.