# 2 Types of Encryption Algorithms

Symmetric - encryption and decryption keys are the same

Asymmetric - (aka public key) - participants have a public key and a private key

# Passive Adversary

Observes and records but does not alter information

# Active Adversary

Interacts with ongoing transmissions, by injecting data or altering them or starts new interactions with legitimate parties

# Generic Encryption Notation

Alice encrypts a message using $E_k(m) = c$

Bob decrypts the message using $m = D_{k'}(c)$

# Exhaustive Key Search

Upon intercepting a ciphertext c, is to go through all keys k from the keyspace K, parameterizing D with each k sequentially, computing each $D_k(c)$ and looking for some meaningful result

# Known Plaintext Attack

- Passive
- An adversary tries to recover plaintext (or the key), given access to the ciphertext alone

# Ciphertext only attack

- Passive
- Given access to some ciphertext and its corresponding plaintext adversaries try to recover unknown plaintext
- adversaries try to recover unknown plaintext or the key from further plaintext

# Chosen Plaintext Attack

- Active
- Allow adversaries to choose some amount of plaintext and see the corresponding ciphertext. Allows advanced analysis to defeat weaker algorithms

# Chosen ciphertext attack

- Active
- For a fixed key, attackers can provide ciphertext of their choosing and receive back the corresponding plaintext, try to deduce the secret key or other information sufficient to decrypt new ciphertext

# One-time pad advantages:

it is considered unbreakable, as the key is as long as the original message, it is random and autogenerated, and destroyed after use

# One-time pad disadvantages

The need for absolute synchronization between sender and receiver, the need for an unlimited number of keys, and the pad can only be used once

# One time pads: Why they are not used

The person who is sending the message must send the pad to the receiver securely, and if you have a reliable channel to send the key you might as well skip the one-time pad, and just use that channel

# What are stream ciphers

They turn a fixed-size (symmetric key) into an arbitrary length keystream unpredictable to adversaries
The mapping of the next plaintext bit to ciphertext is a position varying transformation depending on the input key

# When are stream ciphers suitable:

- Suitable when there is a need to encrypt plaintext one bit at a time (ie. when user-typed characters are sent to a secure site in real time)
- Use stream cipher because there is no requirements that the length of the text be a certain size

# Define Encryption

Encryption transforms data (plaintext) into an unintelligible form (ciphertext)

- Is reversible

# Define In-place encryption

- In storage context plaintext can be replaced by ciphertext without requiring additional memory

# Define Length-Preserving

- Ciphertext consumes no more space than plaintext

# What is decryption key?

Allows the recovery of plaintext, using a corresponding decryption algorithm

# Main properties of block ciphers

- Block length
- Key length
- If plaintext block has fewer bits than block length it is padded

# Define Block Cipher

Processes plaintext in fixed length chunks or blocks
Each block is encrypted with a fixed transformation dependent on the key

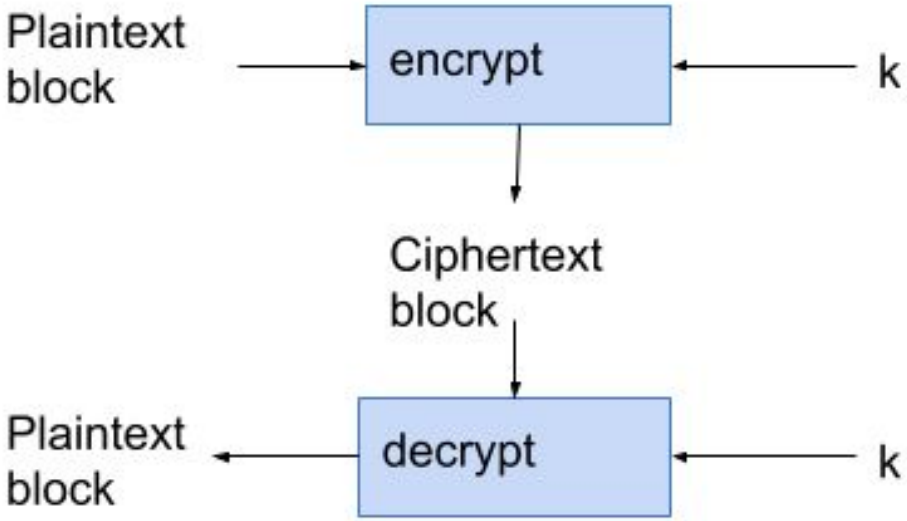
# Block Ciphers: Mode of Operation

combine successive n-bit block operations such that the encryption of one block depends on the other blocks

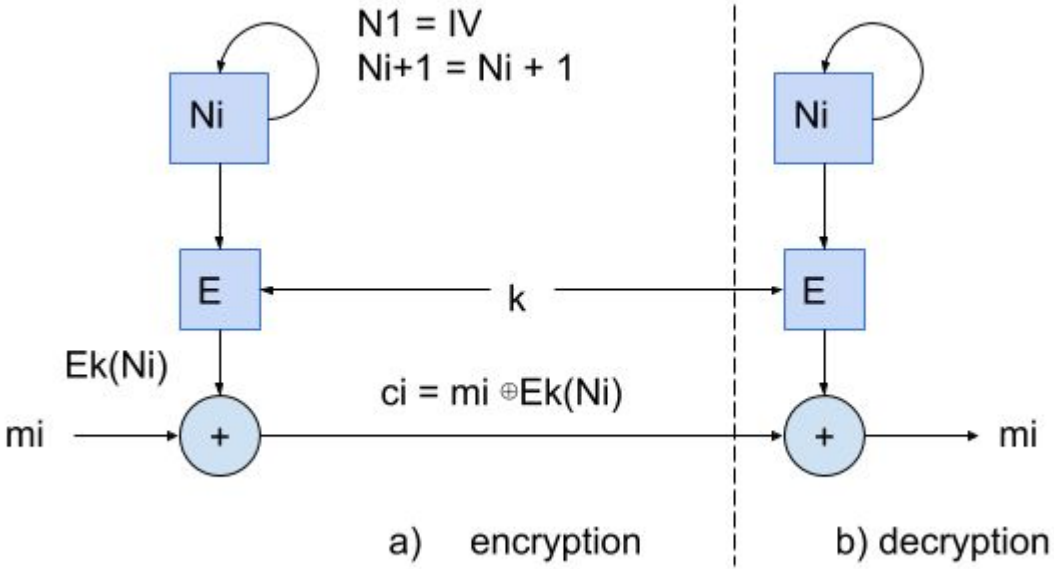
# ECB: Mode of Operation

If a given key k is used to encrypt several identical plaintext blocks m_i then identical ciphertext blocks c_i result ECB does not hide such patterns. This information leak can be addressed by including random bits within a reserved field in each block but it is inefficient and awkward.

# CBC Mode of Operation: Diagram


Plaintext
block
encrypt
k
Ciphertext
block
Plaintext
block
decrypt
k

# CTR Mode of Operation: Diagram


N1 = IV
Ni+1 = Ni + 1
Ni
Ni
E
k
E
Ek(Ni)
ci = mi ⊕Ek(Ni)
mi
+
+
mi
a) encryption
b) decryption

# CTR Mode: How it works

Counter Mode: Message m=m1, m2, ..., mi is encrypted to yield ciphertext c=c1, c2, ..., ci, Blocks mi.ci are n bits.

E denotes a block cipher (encrypt operation) with block length n. CTR mode ECB encrypts an incrementing index (counter) to generate a keystream of blocks to XOR onto corresponding plaintext blocks. To reverse this process, decryption regenerates the same keystream using ECB encryption

# Public Key Encryption: Alice sends a message to Bob

If Alice wants to send a message to Bob using public-key encryption, Bob's public key is used to encrypt and Bob's private key is used to decrypt

# Public Key Signature Scheme: Alice sends a message to Bob

If Alice wants to send a message to Bob using a public-key signature scheme, Alice's private key is used to sign and Alice's public key is used to verify

# Hybrid Encryption

- Symmetric key algorithms are typically faster than public key algorithms
- Public-key methods are more convenient for establishing shared secret keys between endpoints
- Hybrid: To send encrypted messages often between communication endpoints and k is then used in a symmetric-key algorithm for efficient "bulk encryption" of a payload message m

# 3 Security Properties provided by digital signatures

- Data origin authentication
- Data Integrity
- Non-repudiation

# 3 Security Properties provided by digital signatures: data origin authentication

- Assurance of who originated (signed) a message or file

# 3 Security Properties provided by digital signatures: Data Integrity

- Assurance that the received content is the same as that originally assigned

# 3 Security Properties provided by digital signatures: Non-repudiation

- Strong evidence of unique origination making it hard for a party to digitally sign data and later deny having done so.

# 3 Properties of Cryptographic Hash Functions

- Preimage resistance
- Second preimage resistance
- Collision resistance

# 3 Properties of Cryptographic Hash Functions: Preimage Resistance

For all possible hash values h, given h it should be infeasible to find any m such that H(m)=h

# 3 Properties of Cryptographic Hash Functions: Second Preimage Resistance

given any first input m1, it should be infeasible to find any distinct 2nd input m2 such that H(m1)=H(m2)

# 3 Properties of Cryptographic Hash Functions: Collision Resistance

it should be infeasible to find any pair of distinct inputs m1, m2 such that H(m1)=H(m2), (When 2 distinct inputs hash to then same output value, we call it a collision)

# Benefits of encrypt-then-MAC

- Provides integrity of ciphertext
- Plaintext integrity
- If the ciphertext is malleable we do not need to worry b/c MAC will filter out invalid ciphertext
- MAC will not provide any info on the plaintext

# MAC-then-Encrypt: Problems

- No integrity on the ciphertext since we have no way of knowing until we decrypt whether it way authentic or spoofed
- If ciphertext scheme is malleable it may be possible to alter the message to appear valid and have a valid MAC

# MAC-then-Encrypt: Benefits

- Plaintext integrity
- Here the MAC cannot provide any information on the plaintext either since it is encrypted

# MAC-then-encrypt
# Vs
# Encrypt-then-MAC

- Encrypt-then-MAC is generally better
- Any modifications to the ciphertext do not also have a valid MAC and can be filtered out before decryption, protecting against attacks on the implementation
- MAC cannot be used to infer anything about the plaintext

# Symmetric Encryption

- Uses the same key for both encryption and decryption

# Symmetric Encryption: Encryption

- Encryption: takes plaintext and key and provides the ciphertext using substitution and permutation

# Symmetric Encryption: Decryption

- Decryption: reverses the encryption process, produces the original plaintext from the key and ciphertext

# Asymmetric Encryption

- uses two keys: one for encryption and the other for decryption. The two keys are paired together mathematically such that if one key encrypts a message a message the other key can decrypt.

# DES (Data Encryption Standard) Key Length

The key is 64 bits (8 bytes) long. For each byte there is 1 parity bit, so the actual value of the key is 56 bits

# DES (Data Encryption Standard) Encryption and Decryption

- DES contains initial and final permutation step that remaps the positions of the bits to achieve diffusion
- Between the permutation, DES performs 16 rounds of operations using 16 48-bit subkeys generated from the original 56 bit key
- For each round the input is the ciphertext from the previous round, and outputs ciphertext for the next round
- Decryption does the same process in reverse

# What is AES?

- Replacement for DES
- block cipher
- Advanced Encryption Standard

# AES Blocklengths

- input plaintext block is 128-bits
- the key length is 128, 192, or 256 bits long
- keys considered long enough to defeat brute force attempts

# Why is AES and improvement over DES

- Key lengths are longer
- Are considered long enough to defeat brute force

# AES Encryption: Step 1

Each block of plaintext that AES operates on is represented as a square matrix called state array

# AES Encryption: Step 2

State array XORed with per-round key before going through multiple rounds of encryption

# AES Encryption: Step 3

Each round the the algorithm perform SubBytes, ShiftRows, and MixColumns on the state array, which represent substitution and permutation

# AES Encryption: Step 4

The transformed state array is XORed with the per-round key and passed as input to the next round

# AES Encryption: Step 5

The final round which excludes MixColumns Operation returns the ciphertext

# AES Decryption

Decryption is the same process as encryption in reverse

# Public Key Signatures

- Verification of Identity and Message Authenticity

To sign message m, Alice uses her signing private key $s_A$ to create a tag $t_A = S_{s_A}(m)$ and sends $(m, t_A)$

Bob receives the message $(m', t'_A)$, and uses Alice's public verification public key $v_A$ to test whether $t'_A$ is a matching tag for $m'$ from Alice by computing $V_{v_A}(m', t'_A)$

This returns valid if a match is confirmed and invalid otherwise