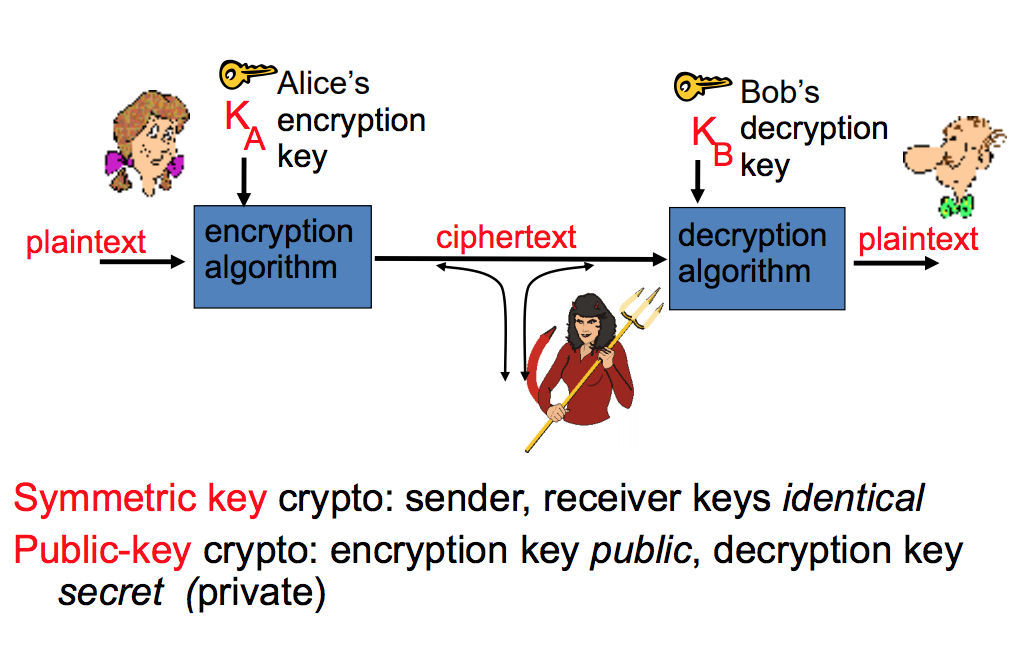
WEEK 3

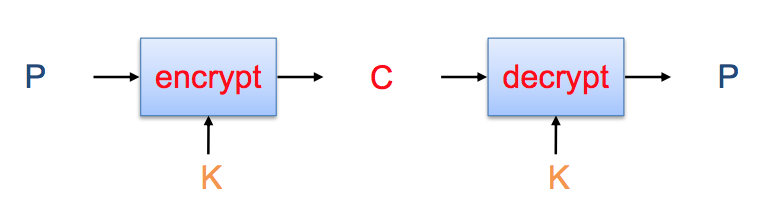
Cryptography

Cryptography (*secret writing*) or **cryptology** is the **practice and study of techniques for secure communication in the presence of third parties called adversaries**.

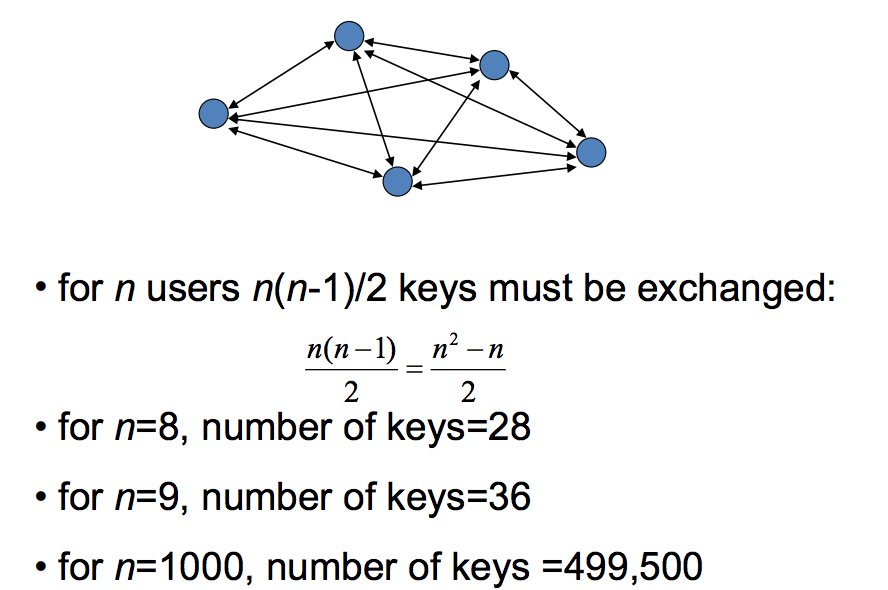
The Language of Cryptography

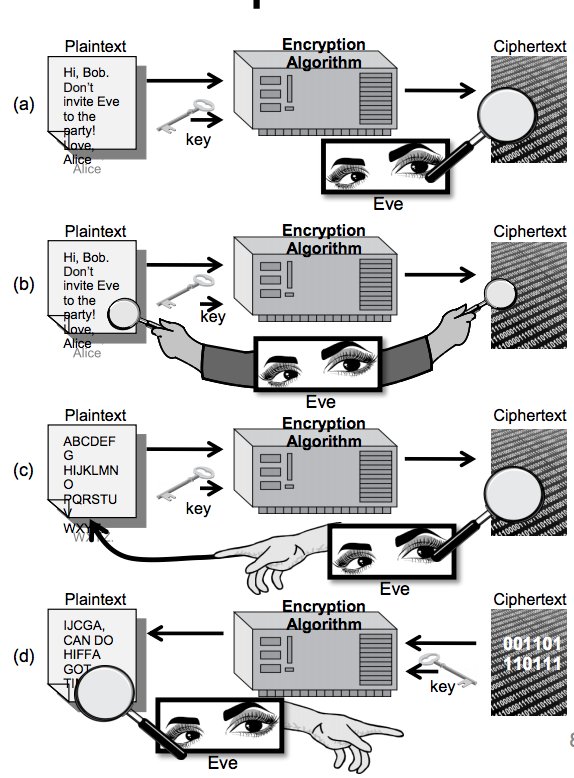


Symmetric Cryptosystem



* Sender Alice wants to send a message (**plaintext P**) to receiver Bob.
* The communication channel is **insecure**.
* If Alice and Bob have previously agreed on a **symmetric encryption scheme** and a **secret key K**, the message can be encrypted (**ciphertext C**).
* ***Limitations of Symmetric Cryptosystems:***
  + Need of a secured channel to exchange the sensitive key information.
  + The ‘n-square’ problem:



Attacks - Attacker’s Capabilities

Attacker may have:

1. Collection of ciphertexts (*ciphertext only attack*)
2. Collection of plaintext/ciphertext pairs (*known plaintext attack*)
3. Collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (*chosen plaintext attack*)
4. Collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (*chosen ciphertext attack*)

Brute-Force Attack

Try all possible keys **K** and determine if **DK(C)** is a likely plaintext.

* *Requires some knowledge of the structure of the plaintext.*

Key - sufficiently long random value.

* To make exhaustive search attacks unfeasible.

Weakness of the One-Time-Pad (OTP)

* In spite of their perfect security, **One-Time-Pads** have some **weaknesses**.
* **THE KEY HAS TO BE AS LONG AS THE PLAINTEXT.**
* Keys can **never** be **reused**.
* Repeated use of one-time-pads allowed the US to break some of the communications of Soviet spies during the cold war.

Types of Symmetric Ciphers

**Block Ciphers**

* Operate on chunks of plaintext of specified length.

**Stream Ciphers**

* Operate on one plaintext character at a time.

Terminology

* **Substitution and Permutation:**
  1. **Substitution (*S-box*)**
  2. **Permutation (*P-box*)**
* **Diffusion** 
  1. If we change a single bit of the plaintext, then (*statistically*) half of the bits in the ciphertext should change, and vice versa.
* **Confusion**
  1. Each bit of the ciphertext should depend on **several parts of the key**, obscuring the connections between the two.

Block Ciphers

Data Encryption Standard (DES)

* Developed by IBM and adopted by NIST in 1977.
* 64-bit blocks and 56-bit keys.
* Small key space makes exhaustive search attack feasible since late 90s.

Triple DES (3DES)

* Nested application of DES with three different keys **KA, KB,** and **KC.**
* Effective key length is 168 bits, making exhaustive search attacks unfeasible.
* **C = EKC(DKB(EKA(P))); P = DKA(EKB(DKC(C)))**
* Equivalent to DES when KA=KB=KC (*backward compatible*).

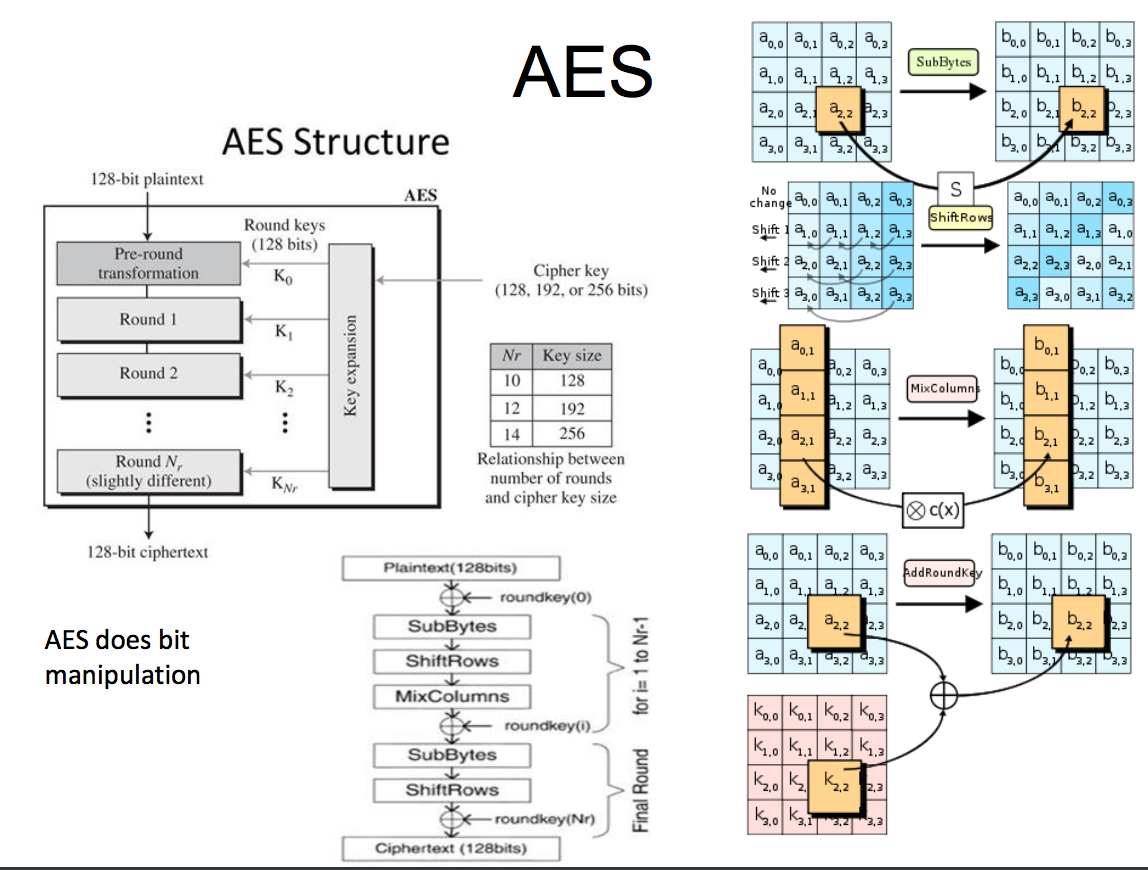
Advanced Encryption Standard (AES)

* Selected by NIST in 2001 through open international competition.
* **128-bit blocks** and several possible key lengths:
  + **128**, **192** and **256** bits.
* Exhaustive search attack not currently possible.
* **AES-256 is the symmetric encryption algorithm of choice.**

Block Size

Normally, the **block size** is fixed, and the block of ciphertext produced by the block cipher is usually also the same length as the plaintext block size.

AES Structure

****

Modes of Operation

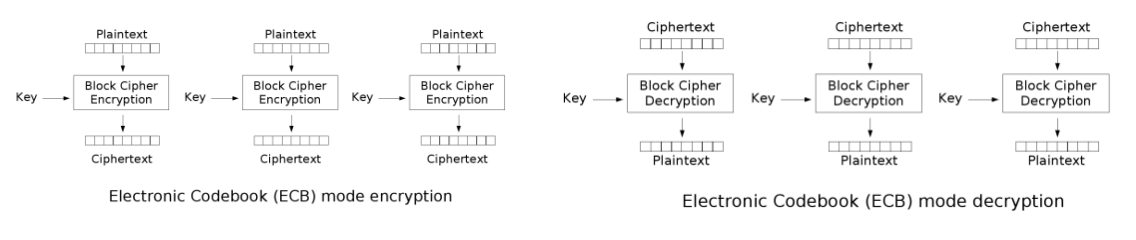
* **Electronic Code Book ECB**
* **Cipher Block Chaining CBC**
* **Cipher Feedback Block CFB**
* **Output Feedback Block OFB**
* **Counter CTR**

Block Cipher Modes

* A **block cipher mode** **describes** the **way** a **block cipher encrypts and decrypts** a **sequence of message blocks**.

Electronic Code Book (ECB)mode ***is the simplest:***

* + Block P[i] **encrypted** into ciphertext block C[i] = EK(P[i])
  + Block C[i] **decrypted** into plaintext block M[i] = DK(C[i])



Strengths and Weaknesses of ECB

**PROS:**

* It’s very **simple**.
* Allows for **parallel encryptions** of the **blocks** of a **plaintext**.
* Can **tolerate** the **loss** or **damage** of a **block**.

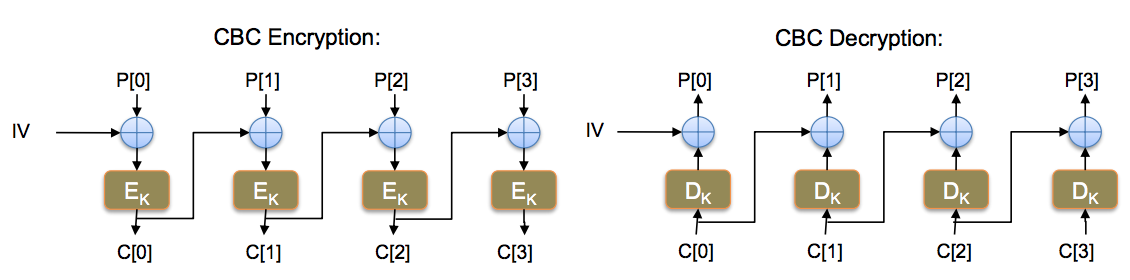
**CONS:**

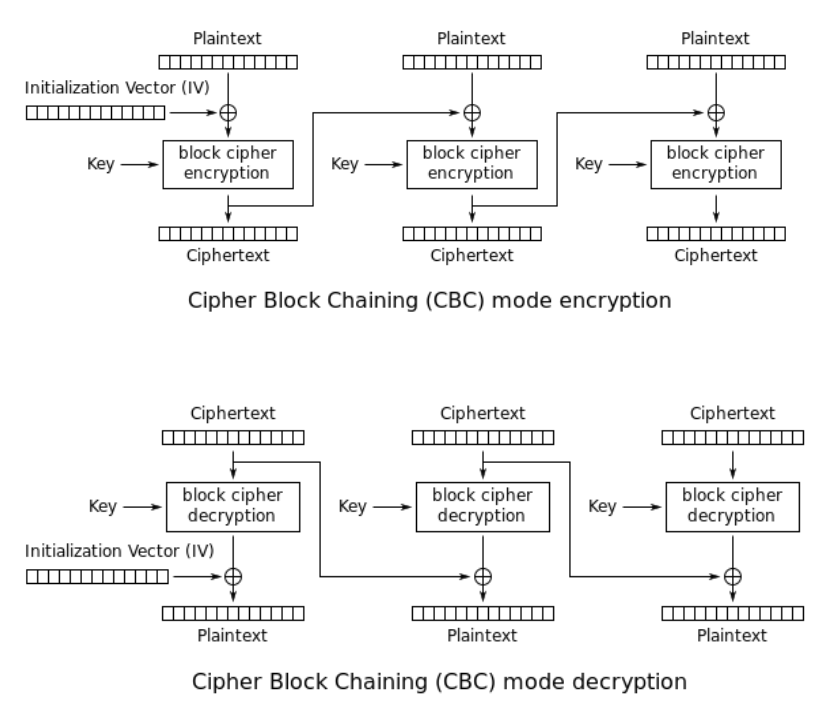
* **Documents** and **images** are **not** **suitable** for ECB encryption since **patterns** in the **plaintext** are **repeated** in the **ciphertext**.

Cipher Block Chaining (CBC) Mode

In **Cipher Block Chaining (CBC**) Mode:

* The previous ciphertext block is combined with the current plaintext block:
  + **C[i] = EK (C[i −1] ⊕ P[i]) – C[−1] = V**
  + a random block separately transmitted encrypted (*known as the initialization vector*)
* Decryption:
  + **P[i] = C[i −1] ⊕ DK (C[i])**





Strengths and Weaknesses of CBC

**PROS:**

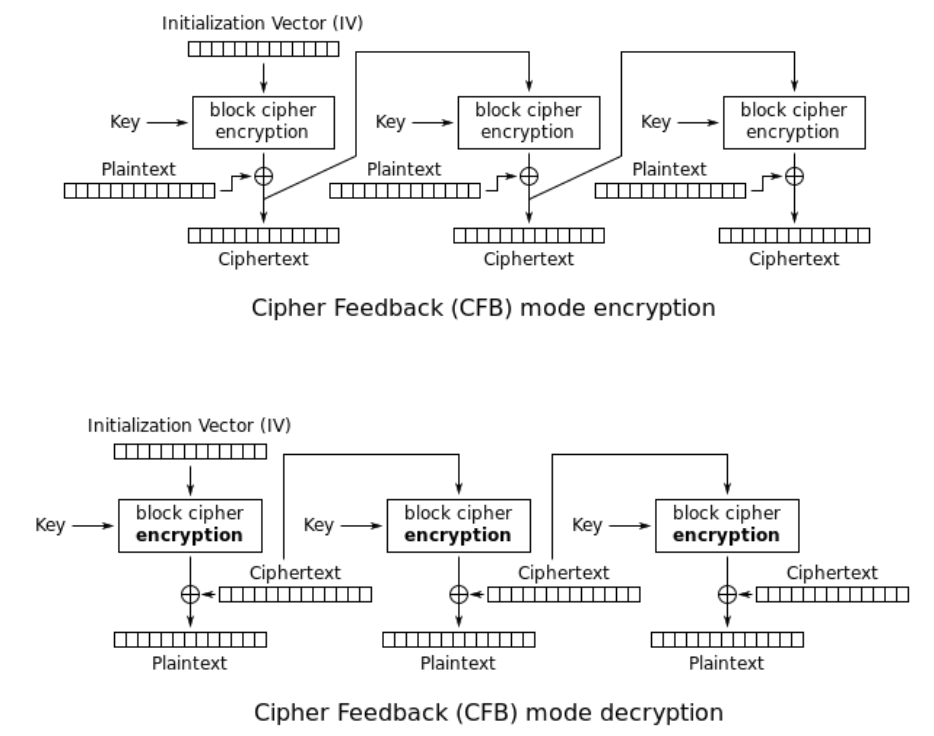
* **Doesn’t show patterns** in the plaintext.
* Is the **most common mode**.
* Is **fast** and **relatively simple**.

**CONS:**

* CBC **requires** the **reliable transmission** of **all** the **blocks**.
* CBC is **not suitable for applications** that **allow packet loss**.
  + *E.g. Music and video streaming.*

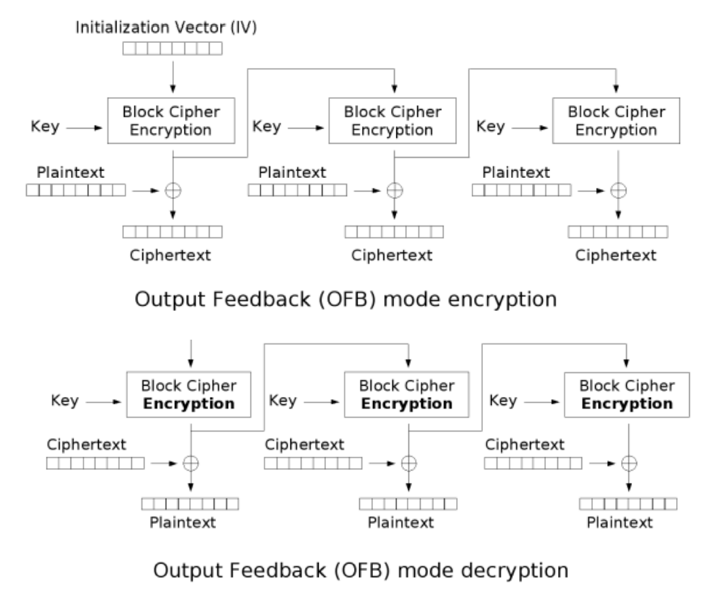
Cipher Feedback Block (CFB) Mode

* Ciphertext feedback (**CFB**) is a mode of operation for a block cipher.
* In contrast to the cipher block chaining (CBC) mode, which encrypts a set number of bits of plaintext at a time, it is at times desirable to encrypt and transfer some plaintext values instantly one at a time, for which ciphertext feedback is a method.
* Like cipher block chaining, ciphertext feedback also makes use of an **initialization vector (IV).** CFB uses a block cipher as a component of a random number generator.
* In CFB mode, the previous ciphertext block is encrypted and the output is **XORed** (see XOR) with the **current plaintext block** to **create the current ciphertext block**.
* The **XOR operation conceals plaintext patterns**. Plaintext cannot be directly worked on unless there is retrieval of blocks from either the beginning or end of the ciphertext.

****

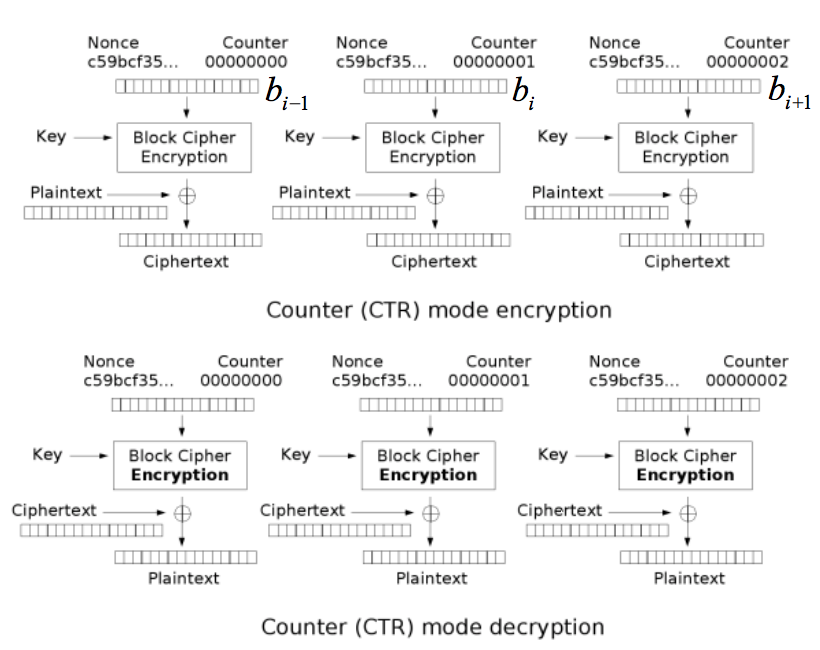
Output Feedback Block (OFB) Mode

* The OFB mode uses an **initial chaining vector (ICV)** in its processing.
* OFB mode **requires** that the **ICV** is a **nonce** (*the ICV must be unique for each execution of the mode under the given key*).
* Each encryption step takes an **input** **block**, **enciphers** it with the **key** provided to **generate** an **output** **block**, and then **exclusive ORs the output block with the plaintext block**.
* The first input block is the ICV and each subsequent input block is the previous output block. The input text can be of any length. The output text will have the same length as the input text.



Counter Mode

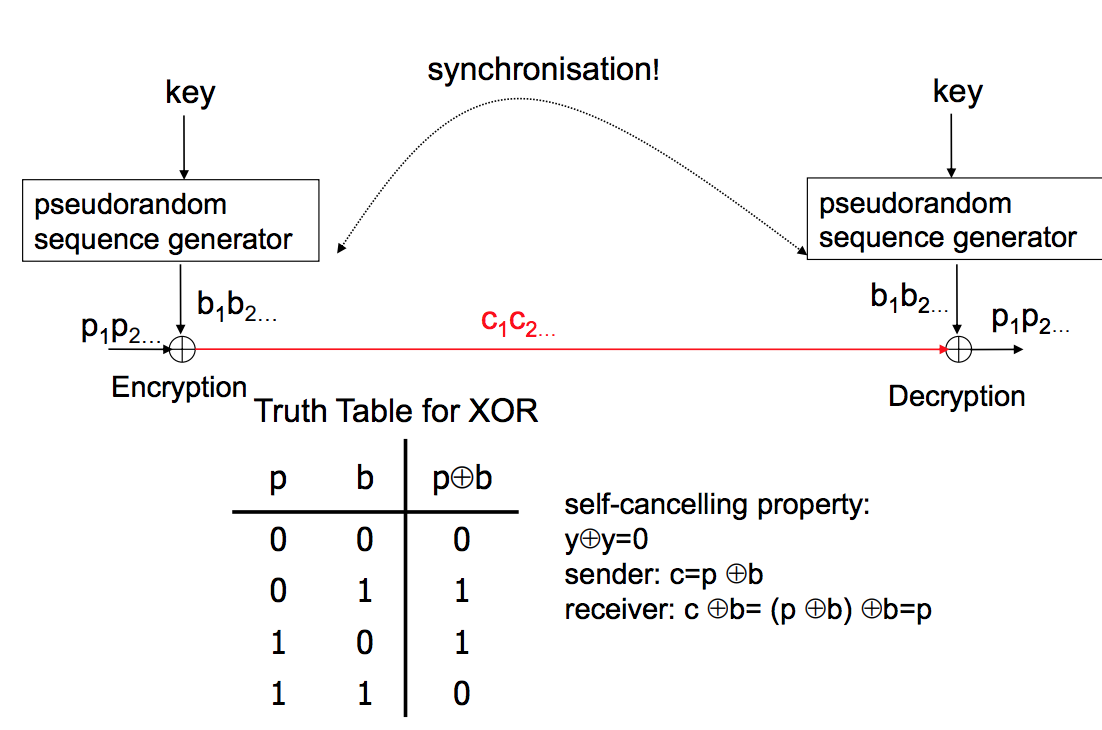
* The Counter Mode or CTR is a simple counter based block cipher implementation.
* Every time a **counter** **initiated** **value** is **encrypted** and **given as input to XOR** with **plaintext** which **results** in **ciphertext** **block**.
* The CTR mode is independent of feedback use and thus can be implemented in parallel.



Characteristics of OFB/CFB/Counter

* Losing Synchronicity in OFB is **fatal**
* All later decryptions will be **garbled** (*blocks will be inserted or removed*).
* **Advantage** OFB does have over CFB:
  + Can **pre-generate** the **keystream** (*and pass to the next block*), since it does not depend on the plaintext.
* **CBC** vs. **CFB**
  + Encryption mode for decryption:  
    Counter mode lets you generate a bit in the middle of the stream.
* **CTR**, **CFB** and **OFB convert block cipher into stream cipher**.

Steam Ciphers



**Strengths**:

* High **speed.**

**Weaknesses**:

* Low **security.**
* **Synchronisation** **issues**.

**Applications**:

* Video data encryption.
* Mobile communications.
* Encrypt satellite communications.

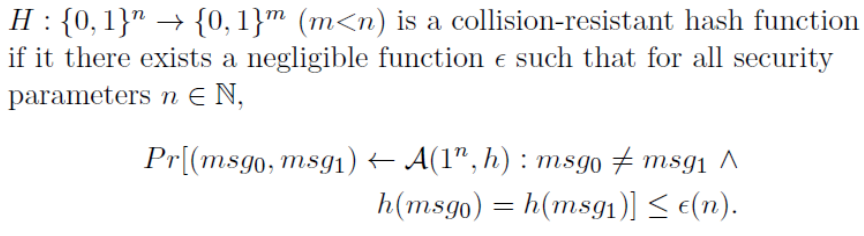
Security Goals and Properties

**Mutual Authentication** The server must **authenticate** the **user** and the user should be able to verify that it is **connected** to the **legitimate** **server**. **Defeats** the **redirection** and **impersonation** **attacks**.

**Perfect Forward Secrecy (PFS)** A scheme **maintains PFS** if **no adversary A** in time **t** can **retrieve** the **past** **session** **keys** **k**, even the long term keys LTK (*i.e., the private key of the user or a session key*) are **compromised**.

**Information Confidentiality** Encrypted message sent by the user must be **indistinguishable** from **randomly** **generated** **messages**, and **supports** **Indistinguishability under Chosen Plaintext Attack (IND-CPA)**.

**Message Integrity** Integrity of each message can be achieved using a well-known **Collision-Resistant Hash Function (CRHF)**.



**Untraceability** Untraceability is maintained if **A cannot distinguish** whether **two generated messages correspond** to the **same** or **two** **different** **identities** of the **users** (*forward untraceability, backward untraceability*).

**Forward privacy** Similar to untraceability with additional capability. **One of two** **messages** is **given** to **adversary** **A**. Clearly, now **A can** **trace** the **user's** **identity** **and**/**or** **other** **information**. **Forward** **privacy** is **maintained** if **A** is **still** **unable** to **trace** **previous** **sessions** (*without giving a secret or session key).*