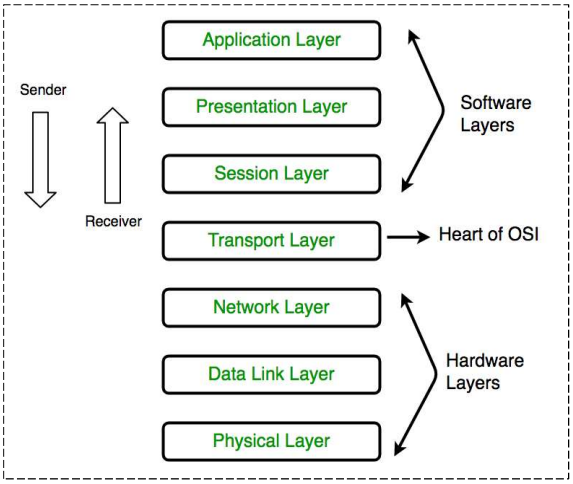
Cryptography Techniques

Professor DR. Bashar Al-Esawi

2022

Cryptography Techniques



TCP/IP MODEL	OSI MODEL
Application Layer	Application Layer
Transport Layer	Presentation Layer
Internet Layer	Session Layer
Network Access Layer	Transport Layer
	Network Layer
	Data Link Layer
	Physical Layer

See also:
https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/?ref=lbp

Types Of Cryptography:

In general there are three types Of cryptography:

1.Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2.Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3.Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Both **Substitution cipher technique** and **Transposition cipher technique** are the types of Traditional cipher which are used to convert the plain text into cipher text.

Substitution Cipher Technique:

In Substitution Cipher Technique plain text characters are replaced with other characters, numbers and symbols as well as in substitution Cipher Technique, character's identity is changed while its position remains unchanged.

Transposition Cipher Technique:

Transposition Cipher Technique rearranges the position of the plain text's characters. In transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

Block Cipher and **Stream Cipher** belongs to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext.

The main difference between a **Block cipher** and a **Stream cipher** is that a block cipher converts the plain text into cipher text by taking plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

1. Monoalphabetic Cipher :

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher :

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

Difference between Confusion and Diffusion

Confusion and **diffusion** area unit the properties for creating a secure cipher. Each Confusion and diffusion area unit wont to stop the secret writing key from its **deduction or ultimately** for preventing the first message.

- ***Confusion is employed for making uninformed cipher text.***
- ***Diffusion is employed for increasing the redundancy of the plain text.***
- The stream cipher solely depends on Confusion,
- Diffusion is employed by each stream and block cipher.

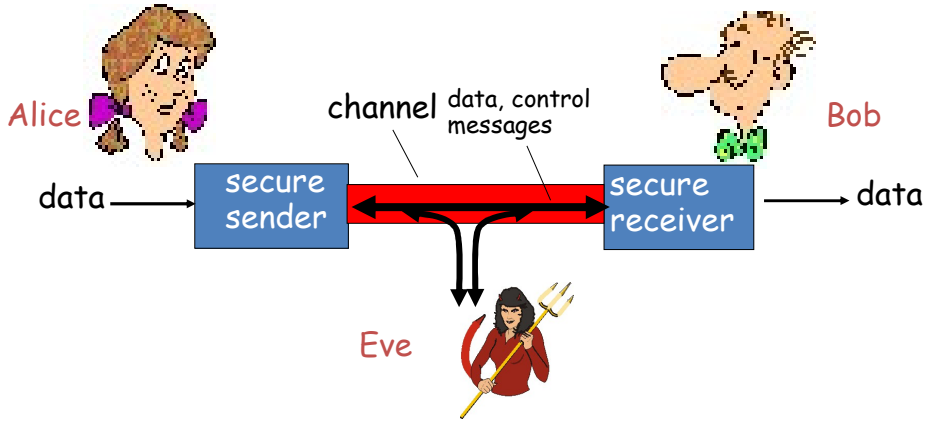
```
Confusion = Substitution
a --> b
Caesar Cipher
Diffusion = Transposition or Permutation
abcd --> dacb
DES
```

Confusion *is an encryption operation where the relationship between key and ciphertext is obscured.*
Diffusion *is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext.*

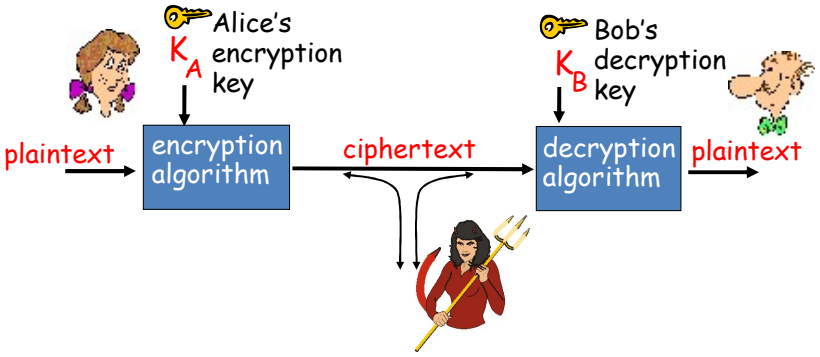
Confusion	Diffusion
Confusion protect the relationship between the ciphertext and key.	Diffusion protect the relationship between the ciphertext and plaintext.
If an individual bit in the key is changed, some bits in the ciphertext will also be modified.	If an individual symbol in the plaintext is changed, there are some symbols in the ciphertext will also be changed.
In confusion, the connection between the data of the ciphertext and the value of the encryption is made difficult. It is completed by substitution.	In diffusion, the numerical mechanism of the plaintext is used up into global statistics of the cipher text. This is achieved by permutation.
In confusion, vagueness is enhanced in resultant.	While in diffusion, redundancy is enhanced in resultant.
The relation among the cipher text and the key is concealed by confusion.	The relation among the cipher text and the plain text is concealed by diffusion.

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Eve (or Trudy, intruder) may intercept, delete, add messages



The language of cryptography

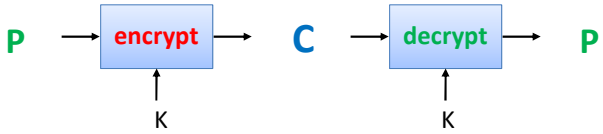


symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret (*private)

Symmetric Cryptosystem

- **Scenario**
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K, the message can be sent encrypted (ciphertext C)
- **Issues**
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?

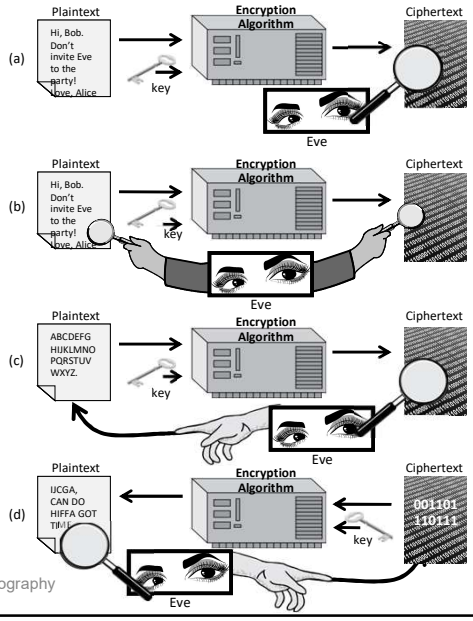


Basics

- **Notation**
  - Secret key K
  - Encryption function $E_K(P)$
  - Decryption function $D_K(C)$
  - Plaintext length typically the same as ciphertext length
  - Encryption and decryption are **one-one mapping functions** on the set of all n-bit arrays
- **Efficiency**
  - functions E_K and D_K should have efficient algorithms
- **Consistency**
  - Decrypting the ciphertext yields the plaintext
  - **$D_K(E_K(P)) = P$**

Attacks

- **Attacker may have**
  a) collection of ciphertexts (**ciphertext only attack**)
  b) collection of plaintext/ciphertext pairs (**known plaintext attack**)
  c) collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (**chosen plaintext attack**)
  d) 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 $D_K(C)$ is a likely plaintext
  - Requires some knowledge of the structure of the plaintext (e.g., PDF file or email message)
- Key should be a sufficiently long random value to make exhaustive search attacks unfeasible

Image by Michael Cote from http://commons.wikimedia.org/wiki/File:Bingo_cards.jpg

Classical Cryptography

- Transposition Cipher
- Substitution Cipher
  - Simple substitution cipher (Caesar cipher)
  - Vigenere cipher
  - One-time pad

https://emn178.github.io/online-tools/sha1.html

Transposition Cipher: rail fence

- Write plaintext in two rows
- Generate ciphertext in column order

- Example: “HELLOWORLD”

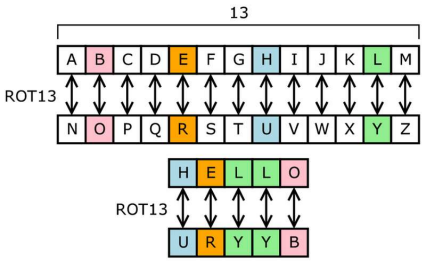
HLOOL
ELWRD
ciphertext: HLOOLELWRD

Problem: does not affect the frequency of individual symbols

Substitution Ciphers

- Each letter is uniquely replaced by another.
- There are 26! possible substitution ciphers for English language.
- There are more than 4.03×10^{26} such ciphers.

- One popular substitution “cipher” for some Internet posts is ROT13.



Public domain image from http://en.wikipedia.org/wiki/File:ROT13.png

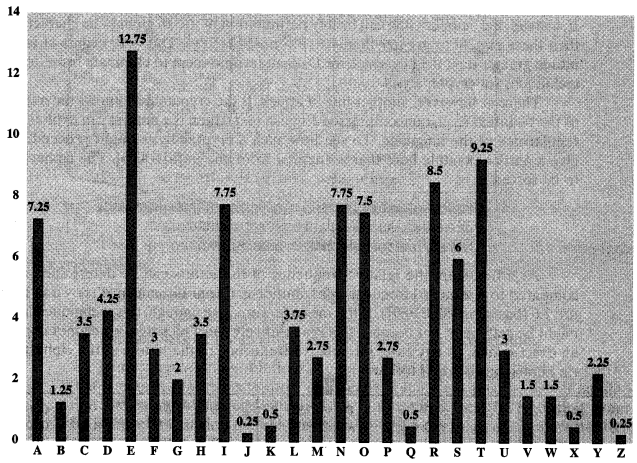
Frequency Analysis

- Letters in a natural language, like English, are not uniformly distributed.
- Knowledge of letter frequencies, including pairs and triples can be used in cryptologic attacks against substitution ciphers.

a:	8.05%	b:	1.67%	c:	2.23%	d:	5.10%
e:	12.22%	f:	2.14%	g:	2.30%	h:	6.62%
i:	6.28%	j:	0.19%	k:	0.95%	l:	4.08%
m:	2.33%	n:	6.95%	o:	7.63%	p:	1.66%
q:	0.06%	r:	5.29%	s:	6.02%	t:	9.67%
u:	2.92%	v:	0.82%	w:	2.60%	x:	0.11%
y:	2.04%	z:	0.06%				

Letter frequencies in the book *The Adventures of Tom Sawyer*, by Twain.

Distribution of Letters in English



Frequency analysis

Simple substitution cipher

substituting one thing for another

– Simplest one: monoalphabetic cipher:

• substitute one letter for another (**Caesar Cipher**)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Example: encrypt "I attack"

Vigenere Cipher

- Idea: Uses Caesar's cipher with various different shifts, in order to hide the distribution of the letters.
- A key defines the shift used in each letter in the text
- A key word is repeated as many times as required to become the same length

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain text: I a t t a c k
Key: 2 3 4 2 3 4 2 (key is "234")
Cipher text: K d x v d g m

Problem of Vigenere Cipher

- Vigenere is easy to break (Kasiski, 1863):
- Assume we know the length of the key. We can organize the ciphertext in rows with the same length of the key. Then, every column can be seen as encrypted using Caesar's cipher.

- The length of the key can be found using several methods:
  - 1. If short, try 1, 2, 3, ...
  - 2. Find repeated strings in the ciphertext. Their distance is expected to be a multiple of the length. Compute the GCD of (most) distances.
  - 3. Use the index of coincidence.

Substitution Boxes

- Substitution can also be done on binary numbers.
- Such substitutions are usually described by substitution boxes, or S-boxes.

	00	01	10	11
00	0011	0100	1111	0001
01	1010	0110	0101	1011
10	1110	1101	0100	0010
11	0111	0000	1001	1100

(a)

	0	1	2	3
0	3	8	15	1
1	10	6	5	11
2	14	13	4	2
3	7	0	9	12

(b)

Figure 8.3: A 4-bit S-box (a) An S-box in binary. (b) The same S-box in decimal. This particular S-box is used in the Serpent cryptosystem, which

Example:

One good example of a fixed table is the S-box from DES (S_5), mapping 6-bit input into a 4-bit output: Given a 6-bit input, the 4-bit output is found by selecting the row using the outer two bits (the first and last bits), and the column using the inner four bits. For example, an input "**011011**" has outer bits "**01**" and inner bits "1101"; the corresponding output would be "1001"

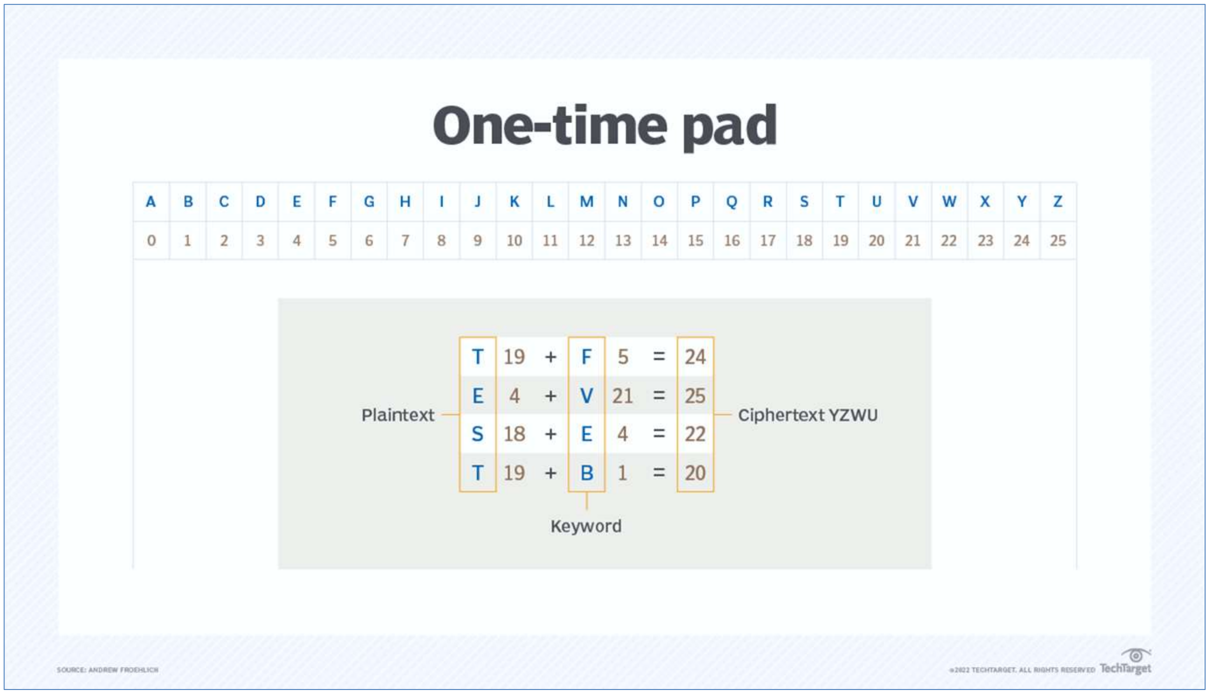
Total Average from (000000)-(111111)

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

https://www.tutorialspoint.com/what-is-s-box-substitution

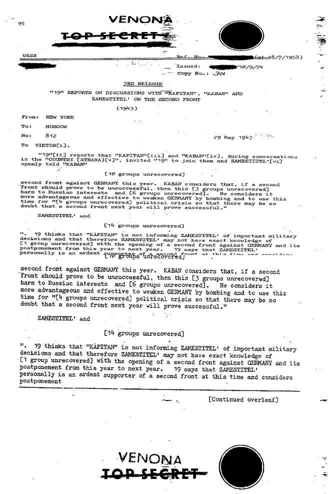
One-Time Pads

- Extended from Vigenère cipher
- There is one type of substitution cipher that is absolutely unbreakable.
  - The **one-time pad** was invented in 1917 by Joseph Mauborgne and Gilbert Vernam
  - We use a block of shift keys, (k_1, k_2, . . . , k_n), to encrypt a plaintext, M, of length n, with each shift key being chosen uniformly at random.
- Since each shift is random, every ciphertext is equally likely for any plaintext.



Weaknesses of the One-Time Pad

- 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 U.S. to break some of the communications of Soviet spies during the Cold War.



VENONA
TOP SECRET
[redacted]

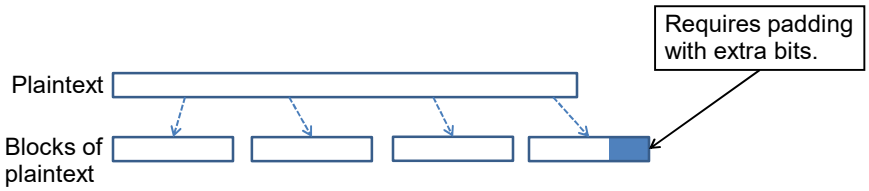
[Continued overleaf]

VENONA
TOP SECRET
[redacted]

Public domain declassified government image from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/venona-soviet-espionage-and-the-american-response-1939-1957/part2.htm

Block Ciphers

- In a **Block cipher:**
  - Plaintext and ciphertext have **fixed length b** (e.g., 128 bits)
  - A plaintext of length n is partitioned into a sequence of m **blocks**, P[0], …, P[m−1], **where $n \leq bm < n + b$**
- Each message is divided into a sequence of blocks and encrypted or decrypted in terms of its blocks.



Padding

- Block ciphers require the length n of the plaintext to be a multiple of the block size b
- Padding the last block needs to be unambiguous (cannot just add zeroes)
- When the block size and plaintext length are a multiple of 8, a common padding method (PKCS5) is a sequence of identical bytes, each indicating the length (in bytes) of the padding
- Example for b = 128 (16 bytes)
  - Plaintext: “Roberto” (7 bytes)
  - Padded plaintext: “Roberto999999999” (16 bytes), where 9 denotes the number and not the character
- **We need to always pad the last block, which may consist only of padding**

Block Ciphers in Practice

- **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
  - $C = E_{KC}(D_{KB}(E_{KA}(P)))$; $P = D_{KA}(E_{KB}(D_{KC}(C)))$
  - Equivalent to DES when KA=KB=KC (backward compatible)
- **Advanced Encryption Standard (AES)**
  - Selected by NIST in 2001 through open international competition and public discussion
  - ***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

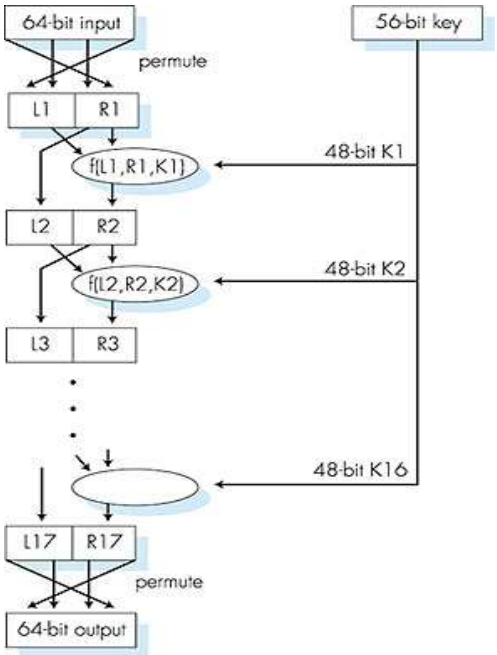
Symmetric key crypto: DES

DES operation

initial permutation

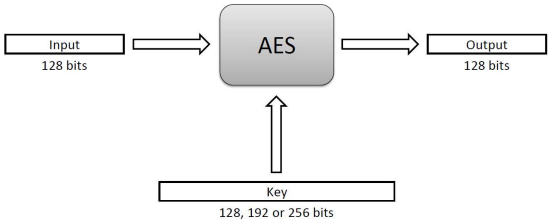
16 identical "rounds" of function application, each using different 48 bits of key

final permutation



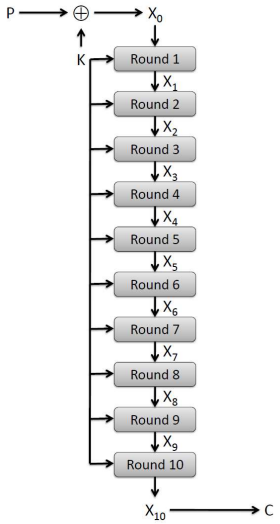
The Advanced Encryption Standard (AES)

- In 1997, the U.S. National Institute for Standards and Technology (NIST) put out a public call for a replacement to DES.
- It narrowed down the list of submissions to five finalists, and ultimately chose an algorithm that is now known as the **Advanced Encryption Standard** (**AES**).
- AES is a block cipher that operates on 128-bit blocks. It is designed to be used with keys that are 128, 192, or 256 bits long, yielding ciphers known as AES-128, AES-192, and AES-256.



AES Round Structure

- The 128-bit version of the AES encryption algorithm proceeds in ten rounds.
- Each round performs an invertible transformation on a 128-bit array, called **state**.
- The initial state X_0 is the XOR of the plaintext P with the key K:
- $X_0 = P \text{ XOR } K$.
- Round i (i = 1, …, 10) receives state X_{i-1} as input and produces state X_i.
- The ciphertext C is the output of the final round: $C = X_{10}$.



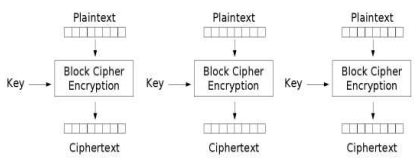
AES Rounds

Each round is built from four basic steps:

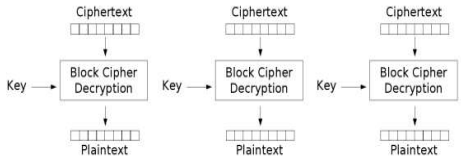
1. **SubBytes step**: an S-box substitution step
2. **ShiftRows step**: a permutation step
3. **MixColumns step**: a matrix multiplication step
4. **AddRoundKey step**: an XOR step with a **round key** derived from the 128-bit encryption key

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 $C[i] = E_K(P[i])$
  - Block C[i] decrypted into plaintext block $M[i] = D_K(C[i])$



Electronic Codebook (ECB) mode encryption

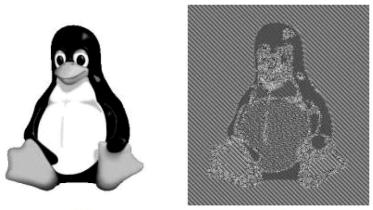


Electronic Codebook (ECB) mode decryption

Strengths and Weaknesses of ECB

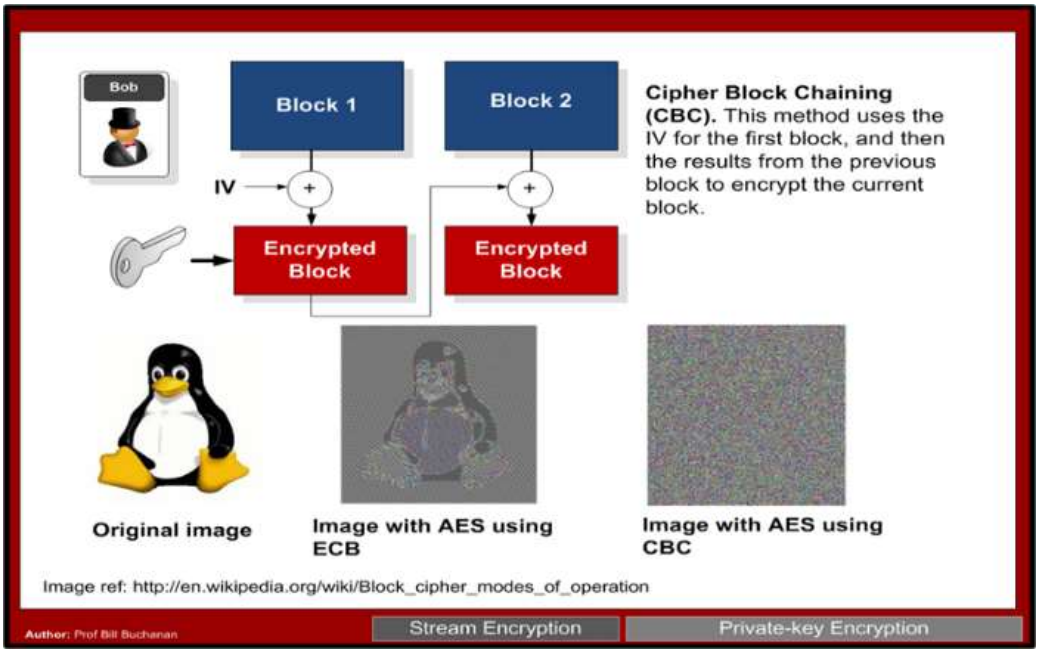
- **Strengths**:
  - Is very simple
  - Allows for parallel encryptions of the blocks of a plaintext
  - Can tolerate the loss or damage of a block

- **Weakness**:
  - Documents and images are not suitable for ECB encryption since patters in the plaintext are repeated in the ciphertext:

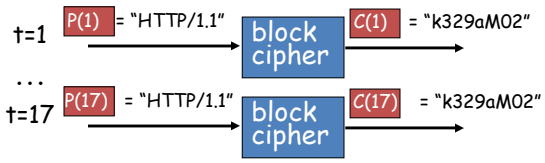


(a) (b)

Figure 8.6: How ECB mode can leave identifiable patterns in a sequence of blocks: (a) An image of Tux the penguin, the Linux mascot. (b) An encryption of the Tux image using ECB mode. (The image in (a) is by Larry Ewing, lewing@isc.tamu.edu, using The Gimp; the image in (b) is by Dr. Juzam. Both are used with permission via attribution.)



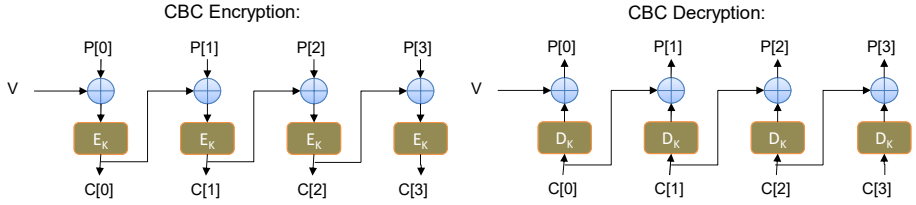
Another Example



https://www.devglan.com/online-tools/aes-encryption-decryption

Cipher Block Chaining (CBC) Mode

- In Cipher Block Chaining (CBC) Mode
  - The previous ciphertext block is combined with the current plaintext block $C[i] = E_K(C[i-1] \oplus P[i])$
  - $C[-1] = V$, a random block separately transmitted encrypted (known as the initialization vector)
  - Decryption: $P[i] = C[i-1] \oplus D_K(C[i])$



Strengths and Weaknesses of CBC

- Strengths:
  - Doesn't show patterns in the plaintext
  - Is the most common mode
  - Is fast and relatively simple
- Weaknesses:
  - CBC requires the reliable transmission of all the blocks sequentially
  - CBC is not suitable for applications that allow packet losses (e.g., music and video streaming)