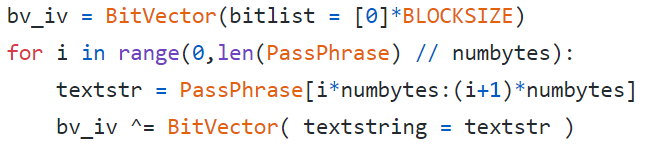
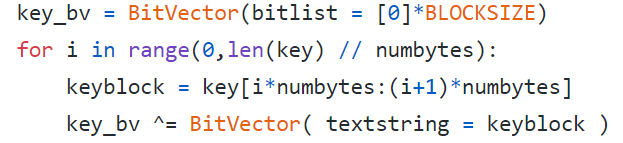
▓differential XORing

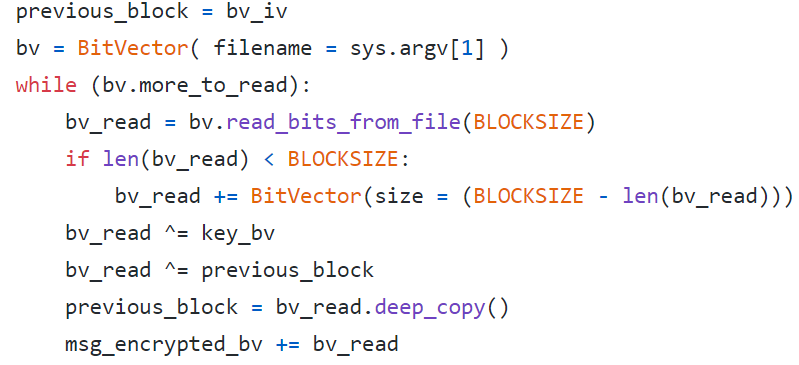
1. Passphrase: a string used as the first “previous encrypted block” for the encryption of first block
2. Algorithm
   1. Encypted
      1. Given: passphrase, blocksize, key
      2. Reduce the passphrase to a bit array of size BLOCKSIZE



* + 1. Reduce the key to a bit array of size BLOCKSIZE



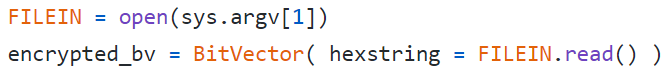
* + 1. Carry out differential XORing of bit blocks and encryption



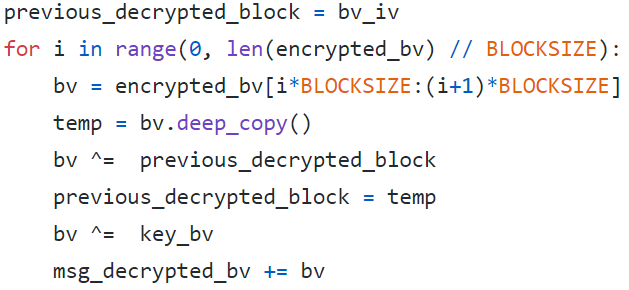
* + 1. Convert the encrypted bitvector into a hex string:



* 1. Decrypted
     1. Given: passphrase, blocksize, key
     2. Reduce the passphrase to a bit array of size BLOCKSIZE:
     3. Create a bitvector from the ciphertext hex string:



* + 1. Reduce the key to a bit array of size BLOCKSIZE
    2. Carry out differential XORing of bit blocks and decryption:



* + 1. Extract plaintext from the decrypted bitvector

▓plaintext: what you want to encrypt

▓ciphertext: The encrypted output

▓enciphering or encryption: The process by which plaintext is converted into ciphertext

▓encryption algorithm: The sequence of data processing steps that go into transforming plaintext into ciphertext. Various parameters used by an encryption algorithm are derived from a secret key. The encryption and decryption algorithms are placed in the public domain. Secret algorithm is less likely to be subject to the same level of testing and scrutiny that a public algorithm is.

▓secret key: used to set some or all of the various parameters used by the encryption algorithm.

* 1. symmetric key cryptography: the same secret key is used for encryption and decryption.
  2. asymmetric key cryptography / public key cryptography: encryption and decryption keys are different, one of them is placed in the public domain.

▓deciphering or decryption: Recovering plaintext from ciphertext

▓decryption algorithm: The sequence of data processing steps that go into transforming ciphertext back into plaintext.

▓cryptography: The many schemes available today for encryption and decryption

▓cryptographic system / cipher: Any single scheme for encryption and decryption

▓block cipher: processes a block of input data at a time and produces a ciphertext block of the same size.

▓stream cipher: encrypts data on the fly, usually one byte at a time.

▓cryptanalysis (breaking the code): relies on a knowledge of the encryption algorithm and some knowledge of the possible structure of the plaintext.

The precise methods used for cryptanalysis depend on whether the attacker has just a piece of ciphertext, or pairs of plaintext and ciphertext, how much structure is possessed by the plaintext, and how much of that structure is known to the attacker.

▓key space: total number of all possible keys that can be used in a cryptographic system. For example, DES uses a 56-bit key. So the key space is of size

▓brute-force attack: When encryption and decryption algorithms are publicly available, a brute-force attack means trying every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

▓codebook attack: mapping from the plaintext symbols to the ciphertext symbols. In a codebook attack, the attacker tries to acquire as many as possible of the mappings between the plaintext symbols and the corresponding ciphertext symbols. You can think of a codebook as the mapping between the plaintext bit blocks and the ciphertext bit blocks, with a ciphertext bit block being related to the corresponding plaintext bit block through an encryption key.

▓algebraic attack: express the plaintext-to-ciphertext relationship as a system of equations. Given a set of (plaintext, ciphertext) pairs, you try to solve the equations for the encryption key.

▓time-memory tradeoff in attacking ciphers: The brute-force and the codebook attacks represent two opposite cases in terms of time versus memory needs of the algorithms. Pure brute-force attacks have very little memory needs, but can require inordinately long times to scan through all possible keys. Codebook attacks can in principle yield results

instantaneously, but their memory needs can be humongously large.

▓time-memory tradeoff attacks: reduce the time taken by a brute-force attack if we use memory to store intermediate results obtained from the current computational steps

▓backdoor: allows an intruder to get inside a networked device without user uthentication credentials. Backdoors may be created by malware or by exploiting vulnerabilities in the security protocols used in a networked device.

▓commercial spyware: application that transmits sensitive information off the device without user consent and does not display a persistent notification that this is happening.

▓denial of service: prevent legitimate users from accessing a network resource. Malware in a machine may turn it into a devicefor mounting a denial-of-service attack on a network resource.

▓hostile downloader: application that is not in itself potentially harmful, but downloads other potentially harmful apps.

▓mobile billing fraud: application that charges the user in an intentionally misleading way.

* 1. sms fraud: application that charges users to send premium SMS without consent, or tries to disguise its SMS activities by hiding disclosure agreements or SMS

messages from the mobile operator notifying the user of charges or confirming subscription.

* 1. call fraud: application that charges users by making calls to premium-rate telephone numbers without user consent.
  2. toll fraud: application that tricks users to subscribe or purchase content via

their mobile phone bill. Toll Fraud includes any type of billing except Premium SMS and premium calls. WAP fraud is one of the most prevalent types of Toll fraud. WAP fraud can include tricking users to click a button on a silently loaded transparent WebView. Upon performing the action, a recurring subscription is initiated, and the confirmation SMS or email is often hijacked to prevent users from noticing the financial transaction.

▓phishing: An application that pretends to come from a trustworthy source, requests a users authentication credentials and/or billing information, and sends the data to a third party.

▓mobile unwanted software (MUwS): application that collects at least one of the following without user consent: ‧ Information about installed applications ‧ Information about third-party accounts ‧ Names of files on the device

▓privilege escalation: application that compromises the integrity of the system by breaking the application sandbox, or changing or disabling access to core security-related functions. Allow an app to steal credentials from other apps and to prevent its own removal. Privilege escalation apps that root devices without user permission are

classified as rooting apps.

* 1. Non-malicious rooting apps: let the user know in advance that they are going to root the device and they do not execute other potentially harmful actions.
  2. Malicious rooting apps: do not inform the user that they will root the device, or they inform the user about the rooting in advance but also execute other harmful actions.

▓ransomware: makes your computer unusable by encrypting all your files

▓spam: unsolicited, unwanted, and frequently annoying email messages that land in your computer or mobile device

▓spyware: application that transmits sensitive information off the device.

▓SSL (Secure Socket Layer) /TLS (Transport Layer Security): certificate based client and

server authentication made possible by the SSL/TLS protocol that makes e-commerce possible. An SSL/TLS certificate for an e-commerce website makes available the public key used by the website.

▓TCP/IP: two different foundational protocols that govern how information is exchanged between two different hosts in the internet. TCP as sitting on top of IP. TCP protocol adds handshaking to this interaction in order to make sure that every data packet sent by a host was actually received by the other host.

▓tor: route anonymizing protocol that makes it easier for folks in countries with heavy censorship and controls to access foreign websites like Google and Facebook.

▓trojan: application that appears to be benign and performs undesirable actions against the user. A trojan will have an innocuous app component and a hidden harmful component.

▓VPN (Virtual Private Network): overlay network that allows a set of hosts to communicate with one another confidentially using IPSec, which is a secure version of the IP protocol.

▓Two building blocks of all classical encryption techniques are substitution and transposition.

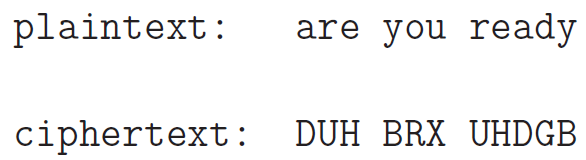
* 1. Substitution: replacing an element of the plaintext with an element of ciphertext. The same overall substitution rule may be applied to every element of the plaintext, or the substitution rule may vary from position to position in the plaintext.
  2. Transposition/permutation: rearranging the order of appearance of the elements of the plaintext. Transposition may be carried out after or before substitution

▓CAESAR CIPHER (Substitution): Each character of a message is replaced by a haracter x position down in the alphabet. Encryption and decryption formula for replacing each character p of the plaintext with a character c of the ciphertext can be expressed as: (k

would be the secret key)





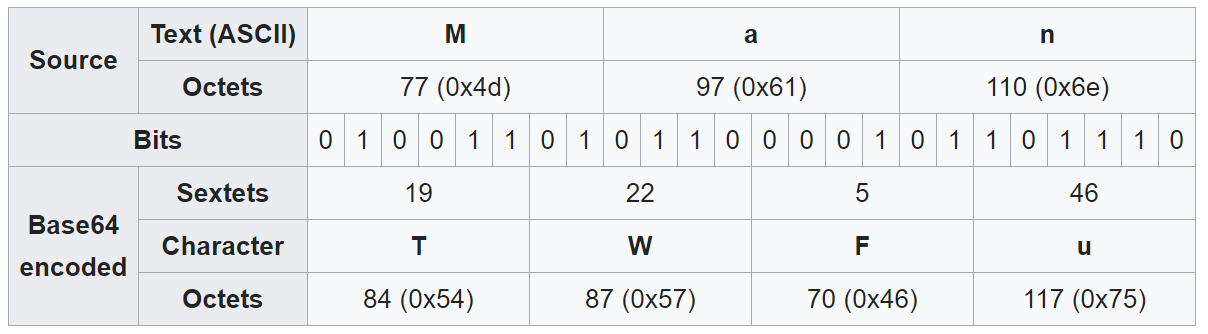


▓save "hello" as a file, the file will have 6 bytes. Due to the new line added before EOF

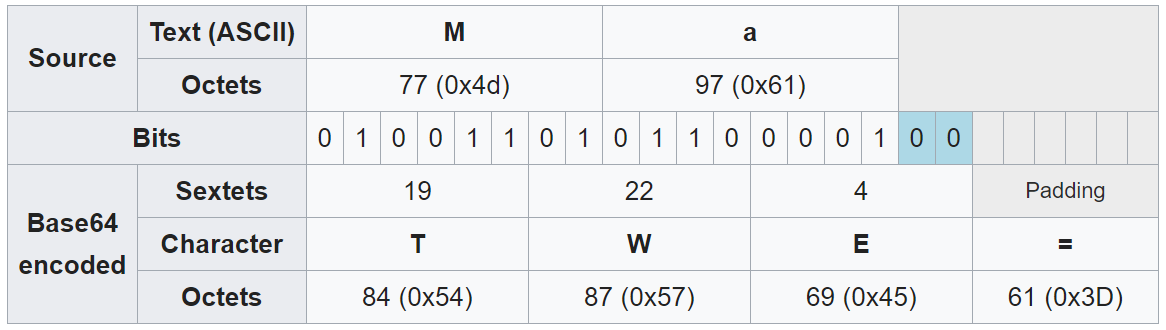
▓Base64 encoding: replaced every consecutive 6 bits with one of 64 possible cipher

Characters (3 bytes into 4 64-base characters as printable characters). Non-printable character are control characters so cannot be used.

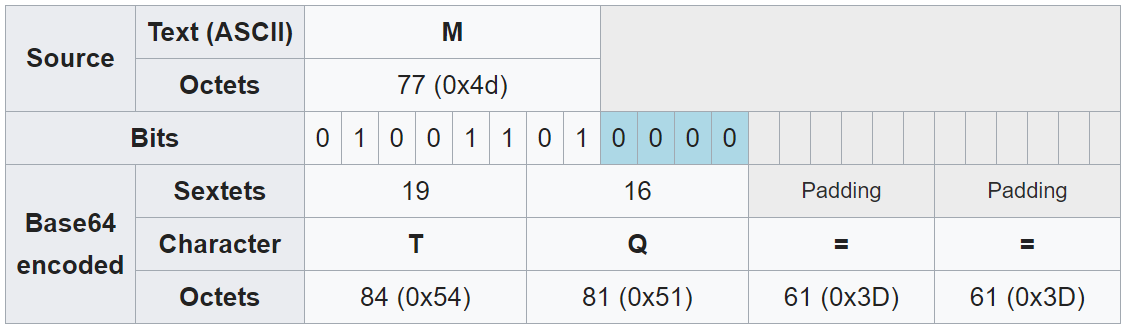
characters *M*, *a*, and *n* are stored as the byte values 77, 97, and 110, which are the 8-bit binary values 01001101, 01100001, and 01101110. These three values are joined together into a 24-bit string, producing 010011010110000101101110. Groups of 6 bits (6 bits have a maximum of 26 = 64 different binary values) are [converted into individual numbers](https://en.wikipedia.org/wiki/Binary_number#Counting_in_binary) from left to right (in this case, there are four numbers in a 24-bit string), which are then converted into their corresponding Base64 character values.

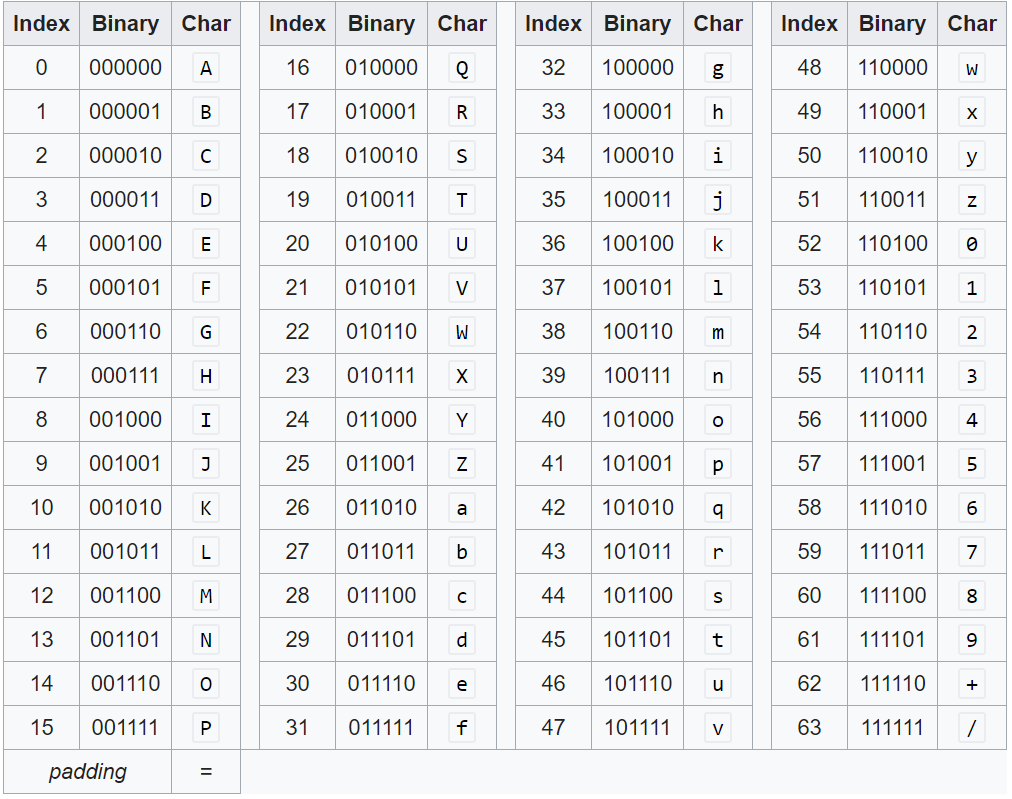


If there are only two significant input octets (e.g., 'Ma'), or when the last input group contains only two octets, all 16 bits will be captured in the first three Base64 digits (18 bits); the two [least significant bits](https://en.wikipedia.org/wiki/Least_significant_bit) of the last content-bearing 6-bit block will turn out to be zero, and discarded on decoding (along with the following = padding characters)



If there is only one significant input octet (e.g., 'M'), or when the last input group contains only one octet, all 8 bits will be captured in the first two Base64 digits (12 bits); the four [least significant bits](https://en.wikipedia.org/wiki/Least_significant_bit) of the last content-bearing 6-bit block will turn out to be zero, and discarded on decoding (along with the following = padding characters):





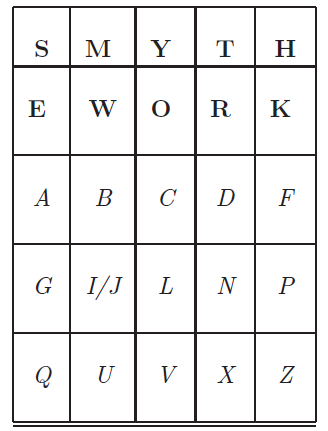
▓When you increase the size of a number by a factor of 10, you are increasing the size by

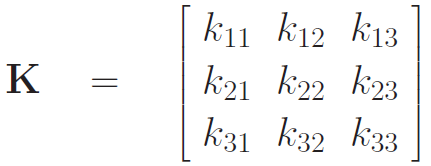
one order ofmmagnitude. So when we say that the keyspace is 10 orders of 10 magnitude larger, that means that the keyspace is larger by a factor of 1

▓monoalphabetic cipher, you use the same substitution rule to find the replacement ciphertext letter for each letter of the alphabet in the plaintext message.

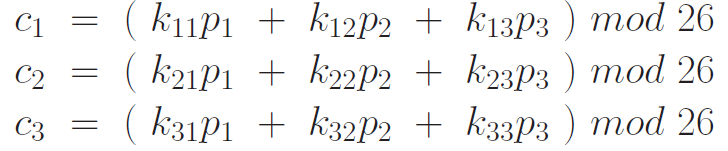
* 1. EX. random permutation, encryption key is the sequence of substitution letters, key space = 26!
  2. any monoalphabetic substitution cipher, regardless of the size of the key space, can be easily broken with a statistical attack.
  3. When the plaintext is plain English, a simple form of statistical attack consists measuring the frequency distribution for single characters, for pairs of characters, for triples of characters, and so on, and comparing those with similar statistics for English.
     1. Equally powerful statistical inferences can be made by comparing the in the cipher relative frequencies for pairs and triples of characters text and the language believed to be used for the plaintext.
     2. Digrams: Pairs of adjacent characters. can represent this table by the joint probability p(x,y) where denotes the first letter of a digram and y the second letter.
     3. Trigrams: triples of characters

▓PLAYFAIR CIPHER (multiple-character substitution)

* 1. Algorithm ()
     1. choose an encryption key, make sure there are no duplicate characters in key. Key = smythework
     2. enter the characters in the key in the cells of a 5\*5 matrix in a left-to-right and top-to-down fashion starting with the first cell at the top-left corner.
     3. fill the rest of the cells of the matrix with the remaining characters in the alphabet and do so in alphabetic order.
     4. for any given pair of plaintext characters, you use the following three rules to determine the corresponding pair of ciphertext characters:
        1. Two plaintext letters that fall in the same row: replaced by letters to the right of each in the row. “bf”-> “ CA”
        2. Two plaintext letters that fall in the same column: replaced by the letters just below them in the column. “ol” -> “CV”
        3. Otherwise, for each plaintext letter in a pair, replace it with the letter that is in the same row but in the column of the other letter. “gf”-> “PA”
     5. Before the substitution rules are applied, you must insert a chosen filler letter (let say it is x) between any repeating letters in the plaintext. So a plaintext word such as “hurray” becomes “hurxray”.
  2. the cipher does alter the relative frequencies associated with the individual letters and with digrams and with trigrams, but not sufficiently
  3. The cryptanalysis of the Playfair cipher is also aided by the fact that a digram and its reverse will encrypt in a similar fashion. That is, if AB encrypts to XY, then BA will encrypt to YX. So by looking for words that begin and end in reversed digrams, EX. receiver, departed, repairer, redder, denuded

▓HILL CIPHER(multiple-character substitution)

* 1. Algorithm:
     1. assign an integer to each letter of the alphabet. Ex. integers 0 through 25 to the letters a through z of the plaintext
     2. encryption key, call it K, consists of a 33 matrix of integers
     3. transform three letters at a time from the plaintext, the letters being represented by the numbers p1, p2, p3 into three ciphertext letters c1, c2, c3



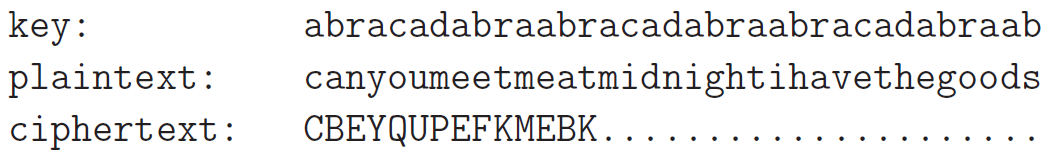
* 1. formula
     1. encryption:
     2. decryption:
  2. keyspace can be made extremely large by choosing the matrix elements from a large set of integers or larger matrices
  3. But it has zero security when the plaintext-ciphertext pairs are known. The key matrix can be calculated easily from a set of known pairs

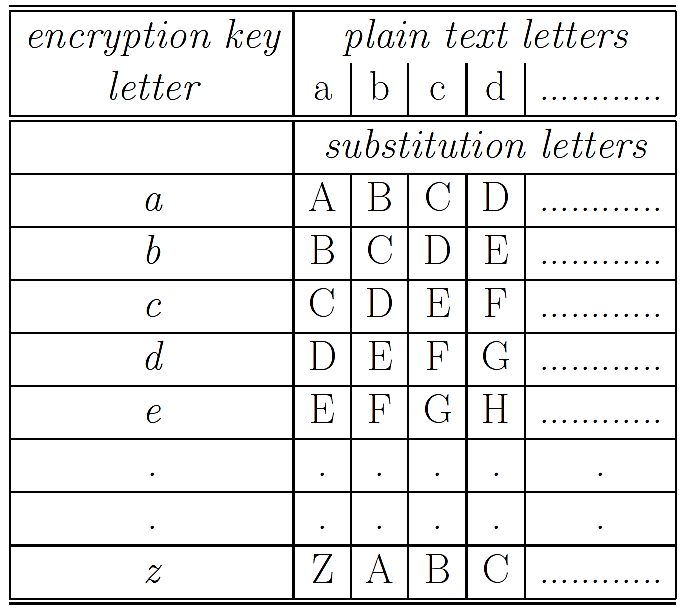
▓monoalphabetic cipher, the same substitution rule is used at every character position in the plaintext message.

▓polyalphabetic cipher: the substitution rule changes continuously from one character position to the next in the plaintext according to the elements of the encryption key.

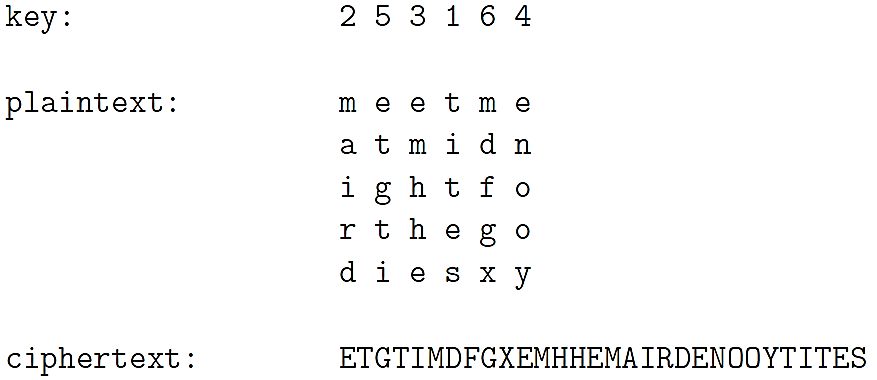
▓Vigenere cipher (polyalphabetic cipher)

* 1. Algorithm: align the encryption key with the plaintext message. Consider each letter of the encryption key denoting a shifted Caesar cipher, the shift orresponding to the letter of the key.





* 1. Since there exist in the output multiple ciphertext letters for each plaintext letter, you would expect that the relative frequency distribution would be effectively destroyed. The longer the encryption key, the greater the masking of the structure of the plaintext. The best possible key is as long as the plaintext message and consists of a purely random permutation of the 26 letters of the alphabet
  2. to break the Vigenere cipher
     1. estimate the length of the encryption key by using Kasiski Examination: examining the ciphertext for sequences of characters that are repeated. The distances between the repeated occurrences of character strings in the ciphertext can serve as possible candidates for the length of the encryption key. If there are several such candidates, one works with the greatest common divisor all possible values as the most likely choice for the key length.
     2. if the estimated length of the key is N, then the cipher consists of N monoalphabetic substitution ciphers and the plaintext letters at positions 1, N, 2N, 3N, etc., will be encoded by the same monoalphabetic cipher.
     3. accumulate the ciphertext characters separately at intervals of N, 2N, 3N, etc., and subject each of the accumulations separately to a statistical analysis.
  3. rotors are used in the electromechanical hardware for implementing a polyalphabetic cipher, such machines are commonly referred to as rotor machine

▓pure permutation cipher: write your plaintext message along the rows of a matrix of some size. You generate ciphertext by reading along the columns. The order in which you read the columns is determined by the encryption key 

▓A, B, and C are bit arrays, ⊕ denotes the XOR operator

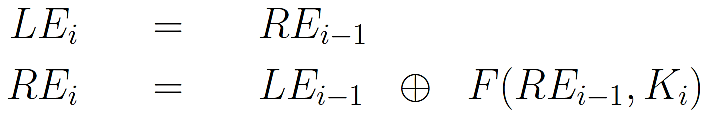
* 1. [A⊕B] ⊕ C = A ⊕ [B⊕C]
  2. A⊕A = 0
  3. A⊕0 = A

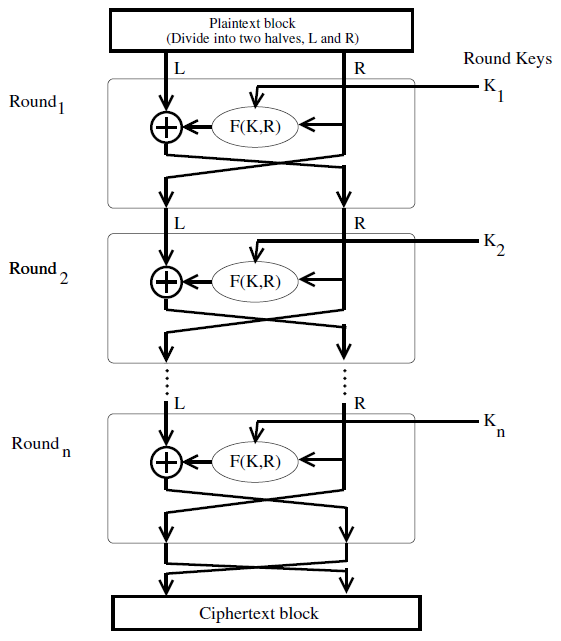
▓ideal block cipher: replace a block of N bits from the plaintext with a block of N bits from the ciphertext.

* 1. the relationship between the input blocks and the output block is completely random. But it must be invertible for decryption to work. Therefore, it has to be one-to-one mapping.
  2. The mapping from the input bit blocks to the output bit blocks can also be construed as a mapping from the integers corresponding to the input bit blocks to the integers corresponding to the output bit blocks. EX. 4-bit is 0~
  3. encryption key for the ideal block cipher is the codebook itself, meaning the table that shows the relationship between the input blocks and the output blocks.
  4. construct the codebook by displaying just the output blocks in the order of the integers corresponding to the input blocks. Ex. 64-bit block -> codebook size (size of the encryption key) is 64\*
  5. The size of the encryption key would make the ideal block cipher an impractical idea. Think of the logistical issues related to the transmission, distribution, and storage of such large keys.

▓Feistel structure consists of multiple rounds of processing of the plaintext, with each round consisting of a substitution step followed by a permutation step.

* 1. Algorithm
     1. input block to each round is divided into two halves L and R.
     2. In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation (Function Feistel) that depends on R and the encryption key.
     3. permutation step at the end of each round consists of swapping the modified L and R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
     4. Feistel Structure: Encryption: relationship between the output of round and the output of the round

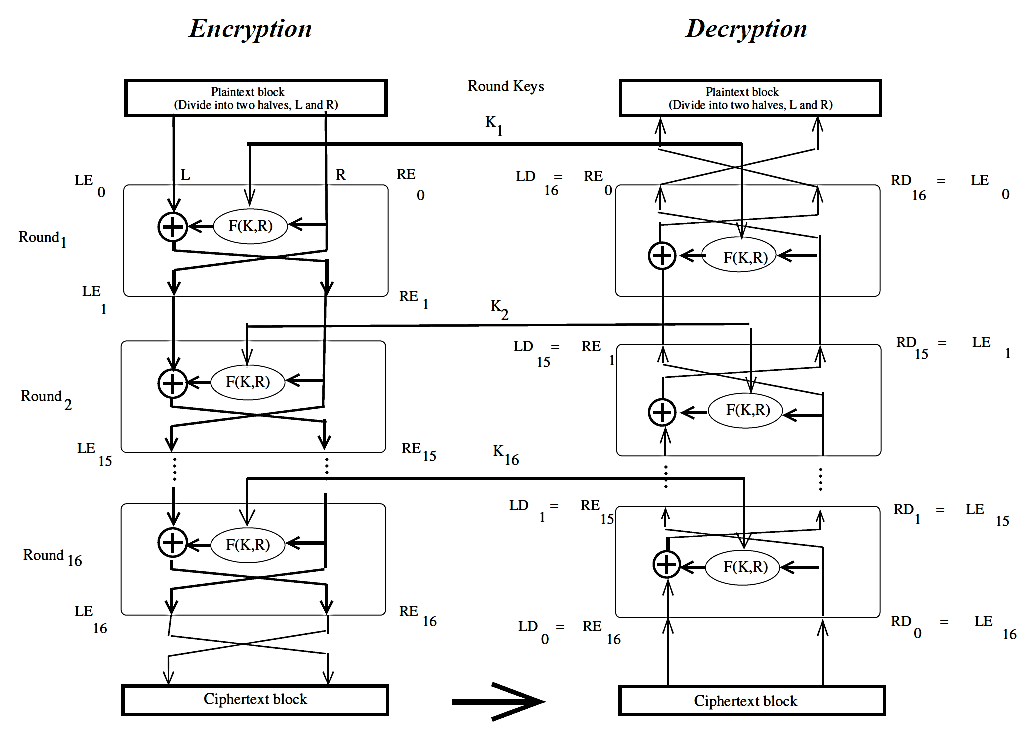


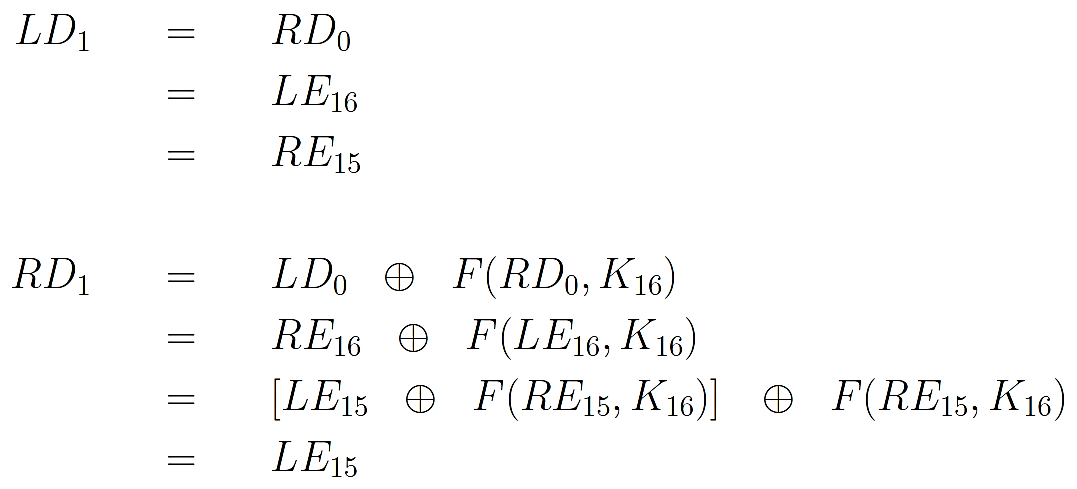


* 1. The output of each round during decryption is the input to the corresponding round during encryption except for the left-right switch between the two halves. The above result is independent of the precise nature of the Feistel function

LD0 = RE16, LE16 = RD0

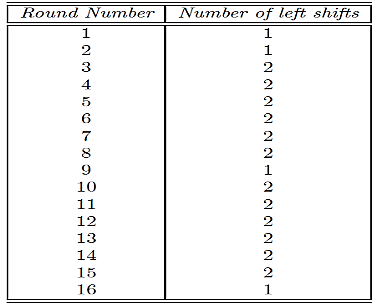
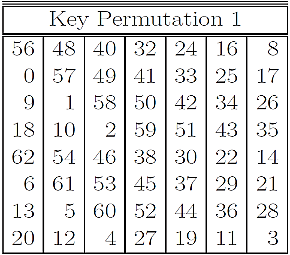
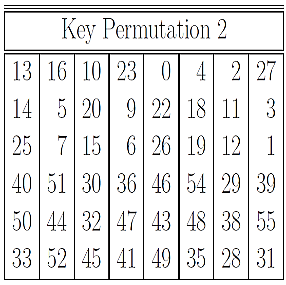
* 1. decryption algorithm is exactly the same as the encryption algorithm with the only difference that the round keys are used in the reverse order. KE1 = KD16

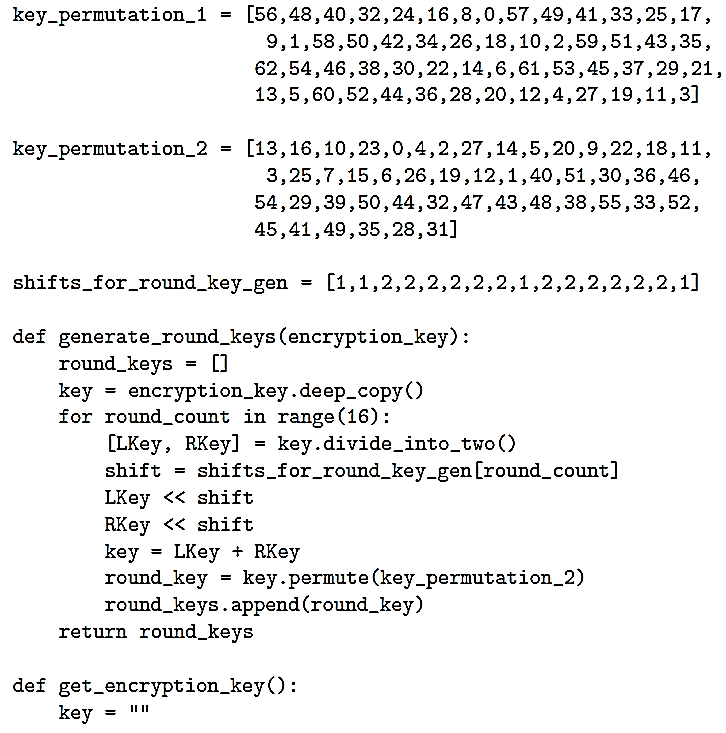


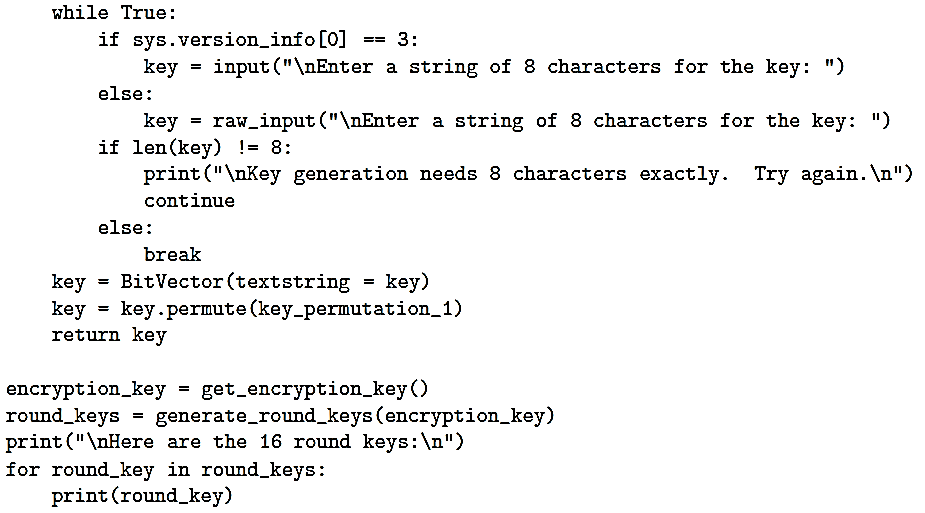


▓DES (Data Encryption Standard): based on Structure Feistel, 16 rounds, 56-bit encryption key (The key itself is specified with 8 bytes, but one bit of each byte is used as

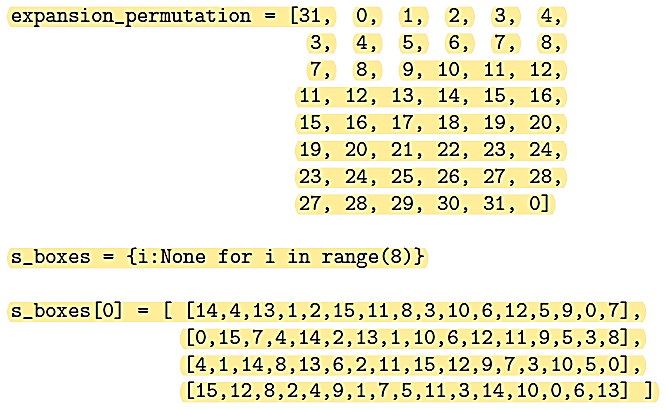
a parity check)

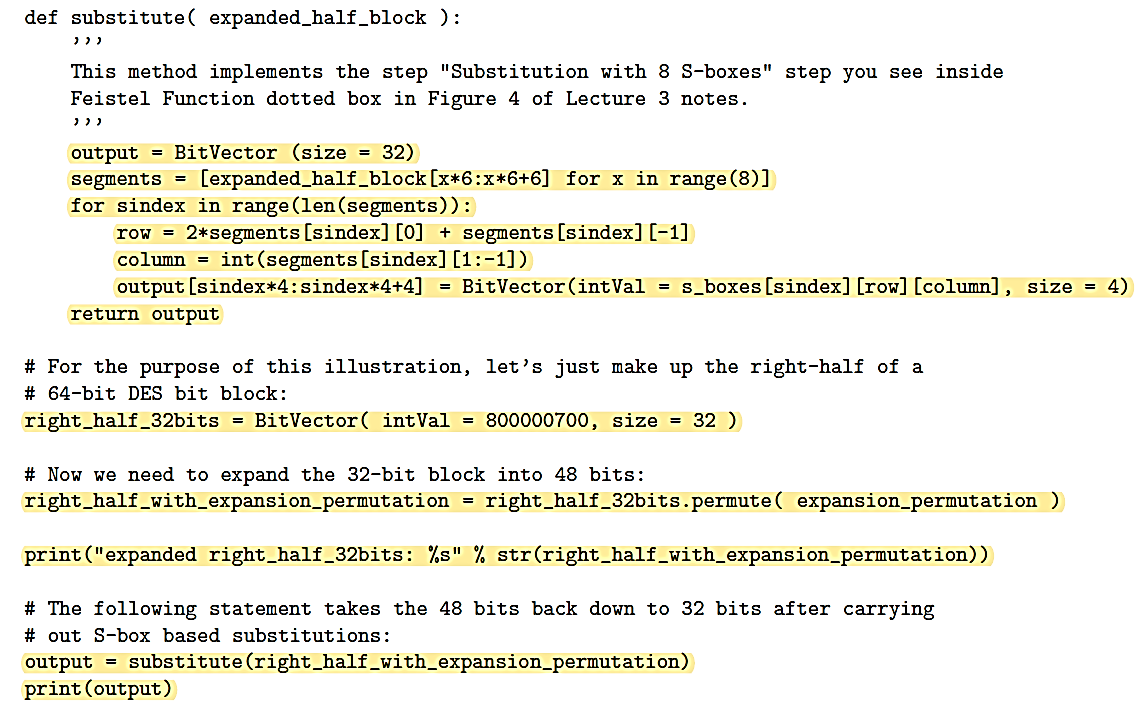
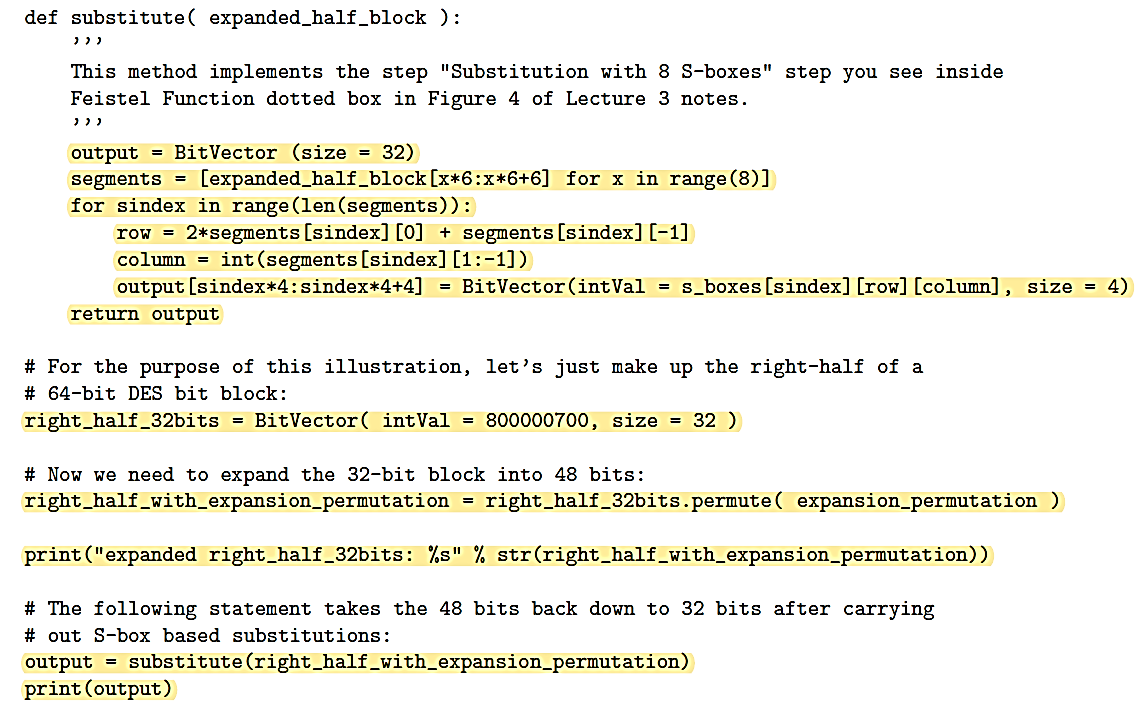
* 1. What is specific to DES is the implementation of the F function in the algorithm and how the round keys are derived from the main encryption key.
  2. DEA (Data Encryption Algorithm): algorithmic implementation of DES
  3. single round of processing in DEA:
     1. expansion permutation (E-step): 32-bit right half of the 64-bit input data block is expanded by into a 48-bit block.
        1. divide the 32-bit block into eight 4-bit words
        2. attach an additional bit on the left to each 4-bit word (last bit of the previous 4-bit word) (circular)
        3. attach an additional bit to the right of each 4-bit word (beginning bit of the next 4-bit word)
     2. 56-bit key is divided into two halves, each half shifted separately, and the combined 56-bit key permuted/contracted to yield a 48-bit round key. To ensure that each bit of the original encryption key is used in roughly 14 of the 16 rounds.
        1. 56-bit encryption key is represented by 8 bytes, with the last bit (the least significant bit) of each byte used as a parity bit.
        2. Encrypt key (Key Permutation 1): Extract the first 7 bits from each of the 8 bytes and permute them in the order of table key\_permutation\_1
        3. Generate round keys:
           1. At the beginning of each round, we divide the 56 relevant key bits into two 28 bit halves and circularly shift to the left each half by one or two bits, depending on the round
           2. join together the two halves and apply a 56-bit to 48-bit contracting permutation. The resulting 48 bits constitute our round key.



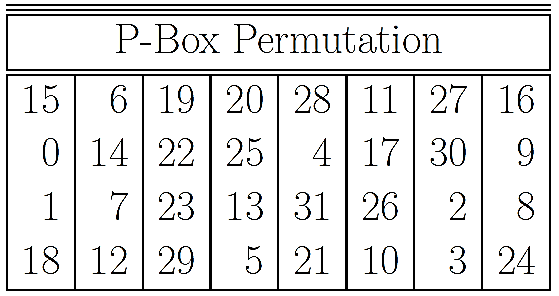


* + - 1. The two halves of the encryption key generated in each round are fed as the two halves going into the next round.
    1. key mixing: 48 bits of the expanded output produced by the E-step are XORed with the round key.
    2. output produced by the previous step is broken into eight six-bit words. Each 6-bit word fed into a separate S-box. Each S-box produces a 4-bit output. Therefore, the 8 S-boxes together generate a 32-bit output
       1. Each of the eight S-boxes consists of a 4\*16 table lookup for an output 4-bit word.
       2. The first and the last bit of the 6-bit input word are decoded into one of 4 rows
       3. the middle 4 bits decoded into one of 16 columns for the table lookup.
       4. This step introduce diffusion in the generation of the output from the input. the row lookup for each of the eight S-boxes becomes a function of the input bits for the previous S-box and the next S-box.



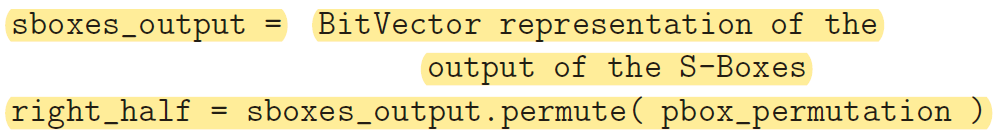


* + - 1. Diffusion: a change in any plaintext bit must propagate out to as many ciphertext bits as possible.
      2. creating the different round keys from the main key is meant to introduce confusion into the encryption process.
      3. Confusion: the relationship between the encryption key and the ciphertext must be as complex as possible. Each bit of the key must affect as many bits as possible of the output ciphertext block.
      4. Diffusion and confusion are the two cornerstones of block cipher design.
    1. 32-bits of the previous step then go through a P-box based permutation

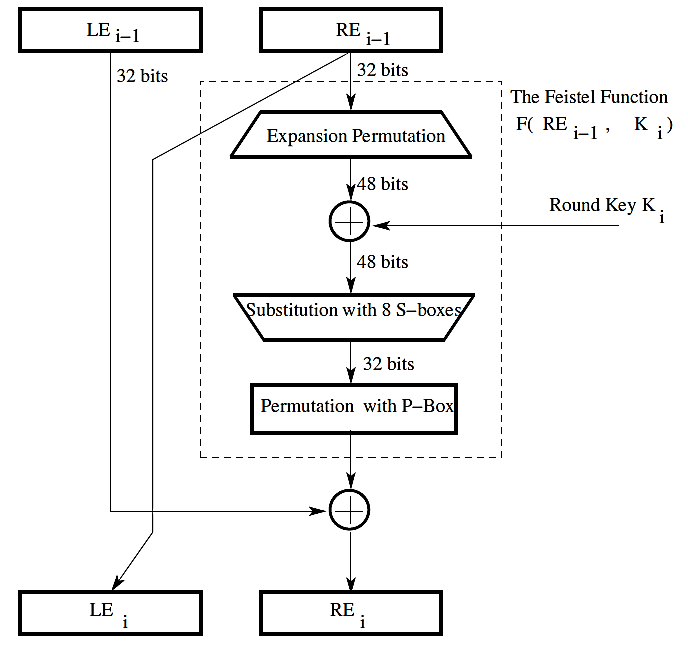


* + - 1. 0th output bit will be the 15th bit of the input, the 1st output bit will be the 6th bit of the input, and so on, for all of the 32 bits. 0th bit of the second output

byte (the 8th bit of the output) will be the 0th bit of the 32-bit input.



* + 1. What comes out of the P-box is then XORed with the left half of the 64-bit block that we started out with. The output of this XORing operation gives us the right half block for the next round.



* 1. WHAT MAKES DES A STRONG CIPHER
     1. The substitution step is very effective as far as diffusion is concerned. if you change just one bit of the 64-bit input data block, on the average it propagates out to affect 34 bits of the ciphertext block.
     2. The manner in which the round keys are generated from the encryption key is also very effective as far as confusion is concerned. if you change just one bit of the encryption key, on the average that affects 35 bits of the ciphertext.
     3. Both effects mentioned above are referred to as the avalanche effect.
     4. 56-bit encryption key means a key space of size

▓In the design of the DES, the S-boxes were tuned to enhance the resistance of DES to what is known as the differential cryptanalysis-attack,

* 1. one plaintext bit block X = [X1,X2, ....,Xn] and corresponding output bit block is Y = [Y1, Y2, ..., Yn].
  2. Y