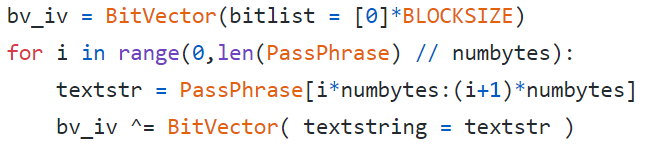
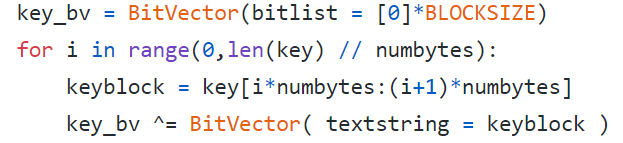
▓differential XORing

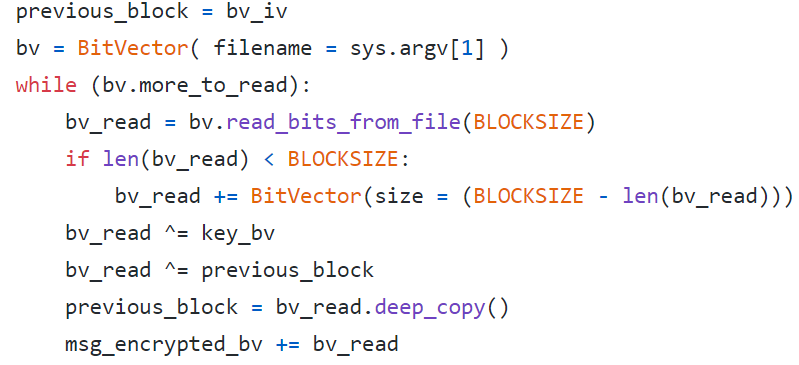
1. Passphrase: a string used as the first “previous encrypted block” for the encryption of first block
2. Algorithm
   1. Encypted
      1. Given: passphrase, blocksize, key
      2. Reduce the passphrase to a bit array of size BLOCKSIZE



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



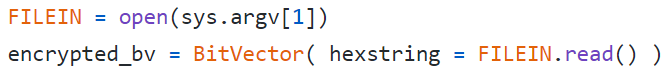
* + 1. Carry out differential XORing of bit blocks and encryption



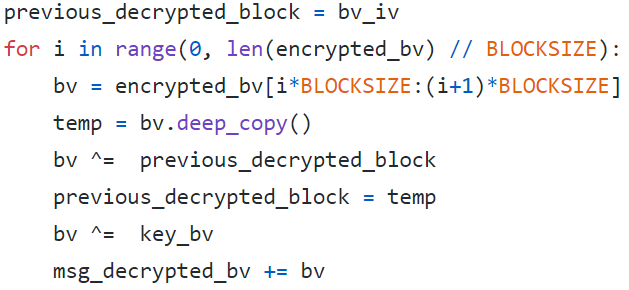
* + 1. Convert the encrypted bitvector into a hex string:



* 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):