CHAPTER 1

Foundations

Terminology

Messages and Encryption

- Plaintext: A message in normal form is Plaintext/Cleartext.

- Ciphertext: A message in encrypted form is Ciphertext.

- Encryption: The process of disguising a message in such a way as to hide its substance is encryption/Encipher (This is ISO term).

- Decryption: The process of turning ciphertext back into plaintext is decryption/Decipher (ISO term).

- Cryptography: The art and science of keeping messages secure is cryptography.

- Cryptographers: The practitioners of cryptography are cryptographers.

Terminology

Messages and Encryption

- Cryptanalysis: The art and science of breaking ciphertext ; that is seeing through the disguise.
- Cryptanalysts: The practitioners of cryptanalysis are cryptanalysts.
- Cryptology: The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology.
- Cryptologists: The practitioners of cryptology are cryptologists.

Terminology

Messages and Encryption

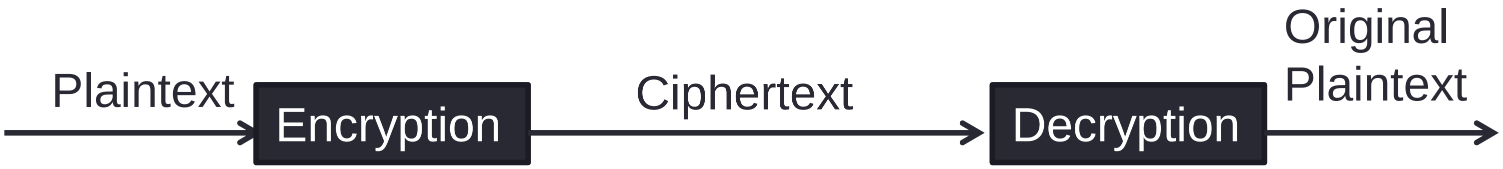
- The plaintext is denoted by M (message) or P (plaintext).
- It can be a stream of bits, text file, bitmap file, a stream of digitized voice, a digital video image etc.
- Ciphertext is denoted by C. The size may be as plaintext or sometimes it can be larger or smaller.
- In mathematical notation:

  E(M)=C where E is encryption function.

  D(C)=M where D is decryption function.
- In any case D(E(M))=M is true.

Terminology

Authentication, Integrity and Nonrepudiation



Encryption and Decryption

In addition to providing confidentiality, cryptography is often asked to do the following:

1. Authentication: The receiver of a message should ascertain its origin.
2. Integrity: The receiver should be able to verify that it has not been modified in transit.
3. Nonrepudiation: A sender should not be able to falsely deny later that he sent a message.

Terminology

Algorithms and Keys

- A cryptographic algorithm (Cipher) is the mathematical function used for Encryption and Decryption.

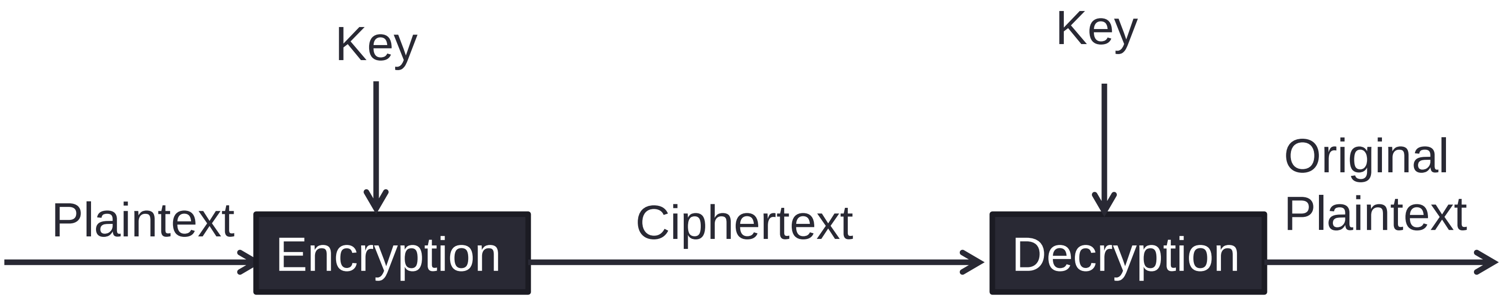
- Restricted Algorithm: If the security of an algorithm is based on keeping the way that algorithm works a secret.
- Drawbacks of Restricted Algorithm:
  1. A large or changing group of users can not use them, because every time a user leaves the group everyone else must switch to a different algorithm.
  2. If someone accidentally reveals the secret, everyone must change their algorithm.
  3. Allow no quality control or standardization.
  4. Every group of users must have their unique algorithm.
  5. Group of users must write their own algorithms and implementations.
  6. If no one in the group is a good cryptographer, then they won’t know if they have a secure algorithm.

Terminology

Algorithms and Keys

- Modern cryptography solves this problem with a key, denoted by k.
- Keyspace: The range of possible values of the key.
- Both encryption and decryption operations use this key.
- The encryption and decryption functions become:

$E_k(M)=C$, $D_k(C)=M$ and $D_k(E_k(M))=M$.



Encryption and Decryption with a Key

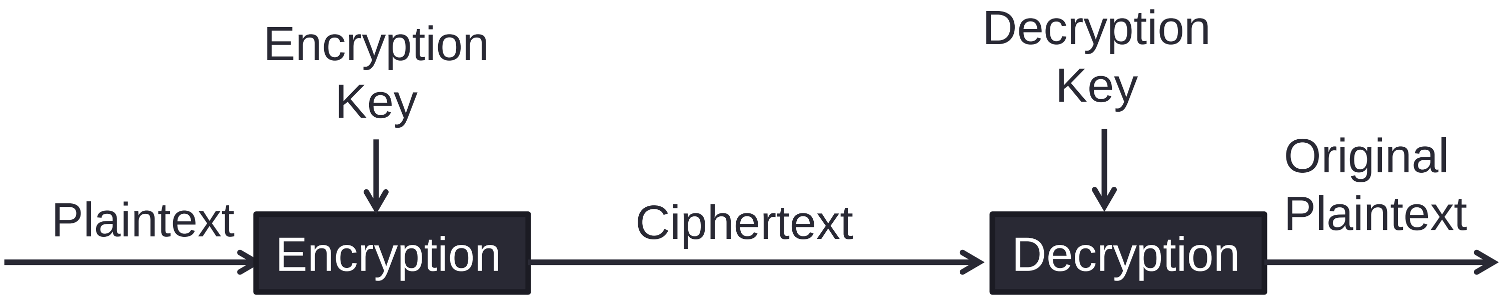
Terminology

Algorithms and Keys

- Some algorithms use a different encryption key and decryption key. In this case:

  $E_{k1}(M)=C$, $D_{k2}(C)=M$ and $D_{k2}(E_{k1}(M))=M$.

- All of the security in these algorithms is based in the key (keys); none is based in the details of the algorithm.



Encryption and Decryption with a Key

Symmetric Algorithm

- Two General Types of key based algorithm:
  - Symmetric Algorithm.
  - Public-key Algorithm.
- In Symmetric key Algorithm encryption key can be calculated from the decryption key and vice versa.
- These algorithms also known as secret key/ single key/ one key or conventional algorithm.
- The sender and the receiver must agree on a key before they can start communication.
- Encryption and Decryption with a symmetric algorithm are denoted by: $E_k(M)=C$, $D_k(C)=M$.

Symmetric Algorithm

- Symmetric algorithms can be divided into two categories.
  - Stream algorithms or Stream Cipher
  - Block algorithms or Block Cipher.
- Stream Cipher operates on the plaintext a single bit (sometimes bytes) at a time.
- Block Cipher operates on the plaintext in group of bits (called blocks) at a time.
- A typical block size is 64 bits.

Public-key Algorithm

- Public-key algorithms also known as Asymmetric algorithm.
- The key used for encryption is different from the key used for decryption.

- These are called public-key algorithm because the encryption key can be made public.

- A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message.

- The encryption key is often called the public key.
- The decryption key is called the private key or secret key.

Cryptanalysis

- The whole point of Cryptography is to keep the plaintext (or the key, or both) secret from eavesdroppers.
- Eavesdroppers also known as Adversaries, Attackers, Interceptors, Interlopers, Intruders, Opponents or Enemy.

- Attack: An attempted cryptanalysis is called an attack.
- There are four general types of cryptanalytic attacks.

- In each of these attacks however it is assumes that the cryptanalyst has complete knowledge of the encryption algorithm used.

Cryptanalysis

1. Ciphertext-only attack: In this case the cryptanalyst has several ciphertext message all of which have been encrypted using the same key. The job is to deduce the key (or keys) used to encrypt or an algorithm to decrypt all new messages encrypted with the same key.

   Given: $C_1=E_k(P_1)$, $C_2=E_k(P_2)$, … $C_i=E_k(P_i)$

   Deduce: Either $P_{1,}$ $P_{2, \dots}$ $P_{i;}$ K, or an algorithm to infer $P_{i+1,}$ from $C_{i+1}=E_k(P_{i+1})$

2. Known-plaintext attack: In this case the cryptanalyst has several ciphertext and their corresponding plaintext. The job is to deduce the key (keys) used to encrypt or an algorithm to decrypt any new message encrypted with the same key.

   Given: $P_{1,}$ $C_1=E_k(P_1)$, $P_{2,}$ $C_2=E_k(P_2)$, … $P_{i,}$ $C_i=E_k(P_i)$

   Deduce: Either K, or an algorithm to infer $P_{i+1,}$ from $C_{i+1}=E_k(P_{i+1})$

Cryptanalysis

3. Chosen-plaintext attack: The cryptanalyst has ciphertext and the associated plaintext. He also chooses the plaintext that gets encrypted. The job is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages.

   Given: $P_{1,}$ $C_1=E_k(P_1)$, $P_{2,}$ $C_2=E_k(P_2)$, … $P_{i,}$ $C_i=E_k(P_i)$ where the cryptanalyst gets to choose P_1, $P_{2, \ldots}P_{i,}$

   Deduce: Either K, or an algorithm to infer $P_{i+1,}$ from $C_{i+1}=E_k(P_{i+1})$

4. Adaptive-chosen-plaintext attack: This is a special case of a chosen plaintext attack. In this case the cryptanalyst can choose the plaintext that is encrypted at the same time he can also modify his choice based on the previous result of encryption.

Security of an Algorithm

- Different algorithm have different degree of security.
- If the cost required to break an algorithm is greater than the value of the encrypted data, then you are probably safe.
- If the time required to break an algorithm is greater than the time the encrypted data must remain secret, then you are probably safe.
- If the amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm, then you are probably safe.
- In fact one-time pad is unbreakable given infinite resources.
- All other cryptosystems are breakable in a ciphertext-only attack, simply by trying every possible key one by one, this is called Brute-force attack.

Other Cryptanalytic Attack

There are at least three other types of cryptanalytic attacks.

5. Chosen-ciphertext attack: The cryptanalyst can choose different cipher text to be decrypted and has access to the decrypted plaintext. The job is to deduce the key.

   Given: $C_{1,}$ $P_1=D_k(C_1)$, $C_{2,}$ $P_2=D_k(C_2)$, …$C_{i,}$ $P_i=D_k(C_i)$

   Deduce: K

   These are applicable to public-key algorithms. Chosen-plaintext and Chosen-ciphertext attack are Chosen-text attack.

6. Chosen-key attack: It means that the cryptanalyst has some knowledge about the relationship between different keys.

7. Rubber-hose cryptanalysis: The cryptanalyst threatens, blackmails, or tortures someone until they give him the key. It is referred to as purchase-key attack.

Substitution Cipher and Transposition Cipher

- In Substitution Cipher, each character in the plaintext is substituted for another character in the Ciphertext. The receiver do inverse operation.
- Four types of Substitution Ciphers are as follows;

1. Simple Substitution or Monoalphabetic Cipher: Each character of the plaintext is replaced with a corresponding character of Ciphertext.

2. Homophonic Substitution Cipher: Like simple substitution cipher, except a single character of plaintext can map to one of several characters of ciphertext. For example “A” could correspond to either 5, 13, 27 or 57, “B” could correspond to either 7, 20, 29 or 51, and so on.

Substitution Cipher

3. Polygram Substitution Cipher: Blocks of characters are encrypted in groups. For example, “ABA” could correspond to “XYZ”, “CDD” could correspond to “SLA” and so on.

4. Polyalphabetic Substitution Cipher: is made up of multiple simple substitution ciphers. For example, there might be five different substitution ciphers used; the particular one used changes with the position of each character of the plaintext.

The famous Caesar Cipher: each character is replaced by the character three to the right modulo 26. For example, “A” is replaced by “D”, “B” is replaced by “E”, …”X” is replaced by “A”, “Y” is replaced by “B” is a simple substitution cipher.

Transposition Cipher

In Transposition Cipher the plaintext remains the same, but the order of characters is shuffle around.

- In a simple columnar transposition cipher, the plaintext is written horizontally onto a piece of graph paper of fixed width and the ciphertext is read vertically.
- For decryption, the opposite procedure is applied with same width (i.e. vertically then horizontally).
- The German ADFGVX cipher: Used during world war I, is a transposition cipher combined with a simple substitution cipher.
- It was very complex algorithm for its day but was broken by Georges Painvin, a French Cryptanalyst.

Transposition Cipher Example

Plaintext: DEPARTMENTOFCOMPUTERSCIENCEANDENGINEERING

D	E	P	A	R	T	M	E	N	T
O	F	C	O	M	P	U	T	E	R
S	C	I	E	N	C	E	A	N	D
E	N	G	I	N	E	E	R	I	N
G									

Ciphertext: DOSEGEFCNPCIGAOEIRMNNTPCEMUEEETARNENITRDN

Double Transposition Cipher

In double Transposition Cipher, the ciphertext (from the plaintext) acts as a plaintext and the corresponding ciphertext is the double transposition ciphertext.

Plaintext: DEPARTMENTOFCOMPUTERSCIENCEANDENGINEERING

Ciphertext: DOSEGEFCNPCIGAOEIRMNNTPCEMUEEETARNENITRDN

D	O	S	E	G	E	F	C	N	P
C	I	G	A	O	E	I	R	M	N
N	T	P	C	E	M	U	E	E	E
T	A	R	N	E	N	I	T	R	D
N									

Double Ciphertext: DCNTNOITASGPREACNGOEEEEMNFIUICRETNMERPNED

ONE-TIME PADS

- One-time pad was invented by Major Joseph Mauborgne and AT&T’s Gilbert Vernam in 1917.
- It is a perfect encryption scheme.
- A one-time pad is nothing more than a large nonrepeating set of truly random key letters, written on sheets of paper, and glued together in a pad.
- The sender uses each key letter on the pad to encrypt exactly one plaintext character.
- Encryption is the modulo 26 of the plaintext character and the one-time pad key character.
- The sender encrypts the message and then destroys the used pages of the pad or used section of the tape.

ONE-TIME PADS

- The receiver has an identical pad and uses each key on the pad in turn, to decrypt each letter of the ciphertext.
- The receiver destroys the same pad pages or tape section after decrypting the message.
- Example: Message: ONETIMEPAD

and the key sequence from the pad is

TBFRGFARFM

Then the ciphertext is IPKLPSFHGO

Because O+T modulo 26=I

N+B modulo 26=P

E+F modulo 26=K etc.

Computer Algorithms

- Many Cryptographic Algorithms. These are three of the most common.

1. DES (Data Encryption Standard): is US and international standard symmetric algorithm (same key is used for encryption and decryption).

2. RSA (Rivest, Shamir and Adleman): is the most popular public-key algorithm, used for both encryption and digital signature.

3. DSA (Digital Signature Algorithm): is another public-key algorithm. It can not be used for encryption, but only for digital signatures.