Introduction to Information Security

Dr. Ashok Kumar Das

Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas
https://sites.google.com/view/iitkgpakdas/

Symmetric-Key Encryption

Symmetric-Key Encryption

Model of conventional encryption

- Consider an encryption scheme consisting of
  - the set of encryption transformations $\{E_e : e \in K\}$
  - the set of corresponding decryption transformations $\{D_d : d \in K\}$, where K is the key space.
- The encryption scheme is said to be S-key or symmetric-key, if for each associated encryption/decryption key pair (e, d), it is computationally "easy" to determine d from e and to determine e from d.
- In most practical symmetric-key encryption schemes, $e = d$.
- Other terms used are single-key, one-key, private-key and conventional encryption.

Symmetric-Key Encryption

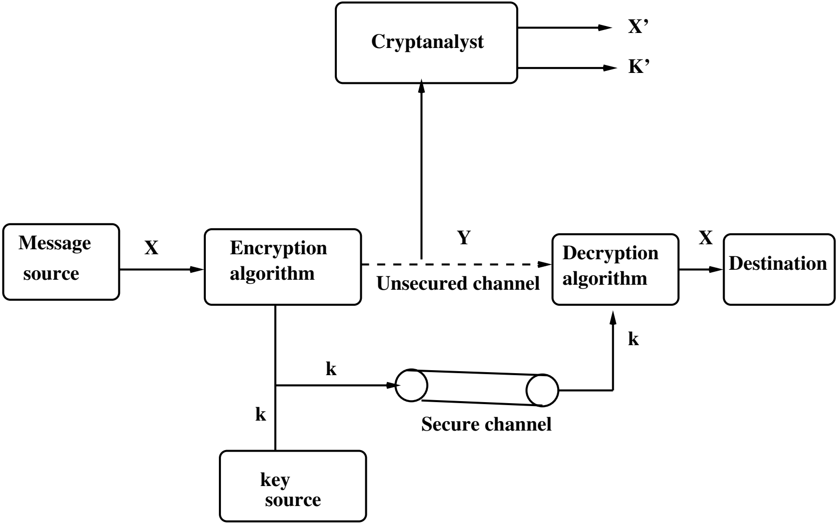

Figure: Model of conventional encryption

Symmetric-Key Encryption

Model of conventional encryption

- With the message $X = [X_1, X_2, \ldots, X_n]$ and the encryption key k as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \ldots, Y_n]$.
- $Y = E_k[X]$
- $Y_i = E_k[X_i]$, for $i = 1, 2, \ldots, n$.
- $X = D_k[Y]$
- $X_i = D_k[Y_i]$, for $i = 1, 2, \ldots, n$.

Symmetric-Key Encryption

Classical Techniques

- There are two classical techniques in conventional or symmetric-key encryption scheme:
  - Substitution Techniques: Involve the substitution of a ciphertext symbol for a plaintext symbol.
  - Transposition Techniques: A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.

Caesar Cipher

- It is the earliest known use of a substitution cipher, and the simplest, was by Julius Caesar.
- Each letter of the alphabet is replaced with the letter standing the three places further down the alphabet.
- For example,
  plaintext: meet me after the new year party
  ciphertext: PHHW PH DIWHU WKH QHZ BHDU SDUWB
- Each letter is wrapped around, so that the letter following *Z* is A. Define the transformation by listing all possibilities as follows.

plaintext:	a	b	c	...	v	w	x	y	z
ciphertext:	D	E	F	...	Y	Z	A	B	C

Symmetric-Key Encryption

Caesar Cipher

- Encoding technique: Let us assign a numerical equivalent to each letter:

a	b	c	...	v	w	x	y	z
0	1	2	...	21	22	23	24	25

- Mathematical model:
  - Encryption: For each plaintext letter p, substitute the ciphertext letter c: $c = E_k(p) = (p + 3) \pmod{26}$, where $k = 3$.
  - Decryption: For each ciphertext letter c, substitute the plaintext letter p: $p = D_k(c) = (c - 3) \pmod{26}$, where $k = 3$.

Symmetric-Key Encryption

The Generalized Caesar Cipher

- A shift may be of any amount, so that the general Caesar algorithm is as follows.
- Mathematical model
  - Encryption: For each plaintext letter p, substitute the ciphertext letter c: $c = E_k(p) = (p + k) \pmod{26}$, where $0 \leq k \leq 25$.
  - Decryption: For each ciphertext letter c, substitute the plaintext letter p: $p = D_k(c) = (c - k) \pmod{26}$, where $0 \leq k \leq 25$.

Symmetric-Key Encryption

Security issues of the Caesar cipher

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed.
- The key space K in this case contains 25 keys, that is $|K| = 25$.
- Attacker simply tries all the 25 possible keys.
- In this case, the attacker could be able to recover the plaintext as well as the encryption key k from the ciphertext easily (It is an example of Ciphertext-only attack (COA)).

Symmetric-Key Encryption

Characteristics of the Caesar cipher

- The encryption an decryption algorithms are known.
- There are only 25 keys to try.
- The language of the plaintext is known and easily recognizable.

Vernam Cipher

- An encryption system was introduced by an AT& T engineer named Gilbert Vernam in 1918.
- He introduced a new parameter (keyword) which is as long as the plaintext and has no statistical relationship to it.
- **Encryption algorithm**
  The system can be expressed as follows:
  $c_i = p_i \oplus k_i$
  where $p_i = i^{th}$ binary digit of plaintext,
  $c_i = i^{th}$ binary digit of ciphertext,
  $k_i = i^{th}$ binary digit of key,
  $\oplus =$ bitwise exclusive-or (XOR) operator.
- **Decryption algorithm**
  Because of the properties of XOR, decryption simply involves the same bitwise operation: $p_i = c_i \oplus k_i$.

Symmetric-Key Encryption

Vernam Cipher

- **Construction of key:**
  - Keyword should be as long as the plaintext and can be repeating.
- Vernam cipher is an example of classical stream cipher.
- It is also called one-time pad, because each plaintext is appended with random key.
- It is proved in the literature that one-time pad is unbreakable (proof will be given mathematically later), since it produces random output that bears NO satistical relationship to the plaintext.

Symmetric-Key Encryption

Vernam Cipher

Problems with the one-time pad

- Generation of key.
- Problem of key distribution and protection.

Because of these difficulties, the one-time is of limited utility, and is used primarily for low-bandwidth channels requiring very high security.