Cryptography (and Information Security)
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 2.3: Characteristics of cryptographic systems &
Symmetric-key encryption

Table of contents I

Three characteristics of cryptographic systems

Cryptographic systems characterized along 3 independent dimensions:

1. Type of operations used to transform plaintext into ciphertext.
2. Number of keys used.
3. Way in which plaintext is processed.

1. Type of operations used to transform plaintext into ciphertext.

- All encryption algorithms are based on two general principles:
  - **Substitution**: each element in plaintext (bit, letter, group of bits or letters) is mapped into another element.
  - **Transposition**: elements in plaintext are rearranged.

  All **operations must be reversible** (so that no information is lost).
- Most systems, referred to as **product systems**, involve multiple stages of substitutions and transpositions.

Three characteristics of cryptographic systems (cont.)

2. Number of keys used.

- **Symmetric, single-key, secret-key, or conventional encryption**: both sender and receiver use “same” key.
- **Asymmetric, two-key, or public-key encryption**: sender and receiver use different keys.

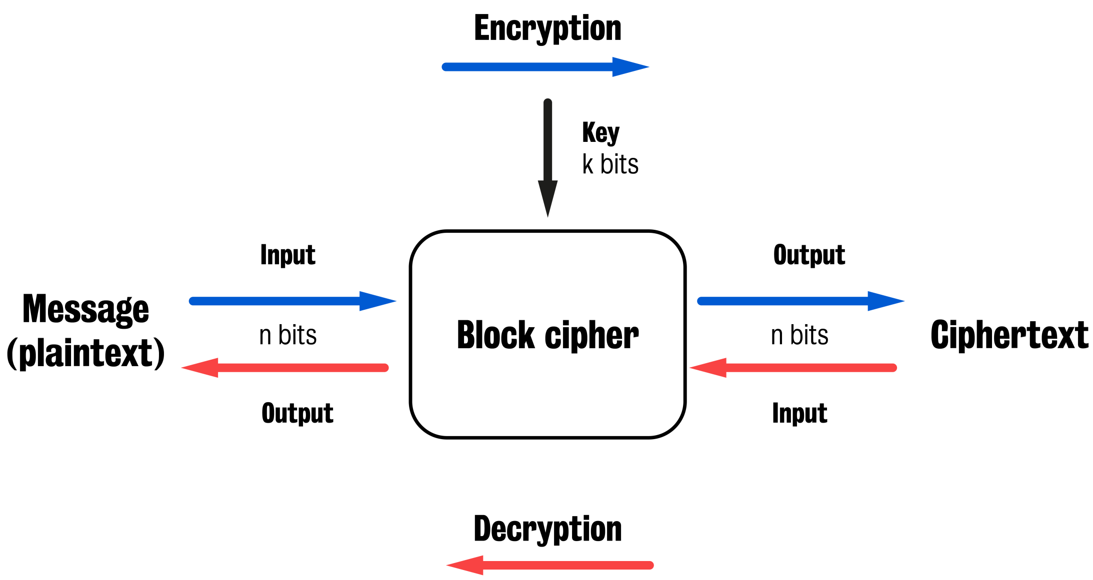
3. Way in which plaintext is processed.

- **Block cipher** processes input one block of elements at a time, producing an output block for each input block.
- **Stream cipher** processes input elements continuously, producing in output one element at a time, as it goes along.

Block ciphers, stream ciphers, and codes

A block cipher is an encryption scheme that breaks up the plaintext message into strings (blocks) of a fixed length n and encrypts one block at a time.

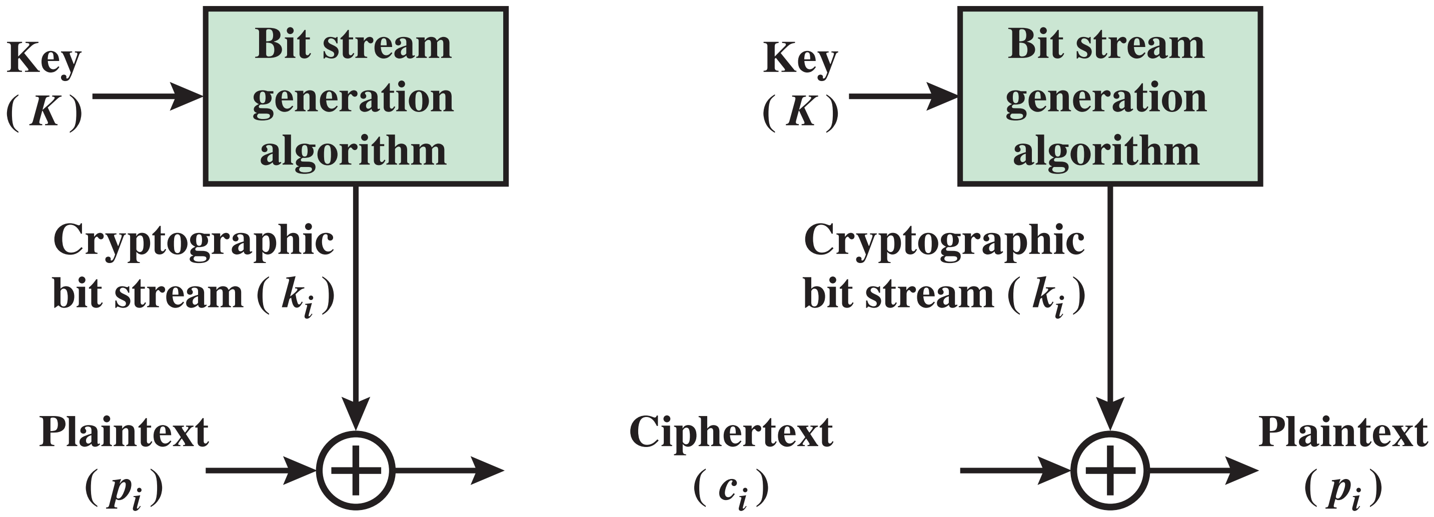
- It takes in input one block of n bits of plaintext and a key of k bits, producing in output one block of ciphertext of n bits.
- For decryption, it takes in input a block of n bits of ciphertext and a key of k bits, producing in output a plaintext block of n bits.



Block ciphers, stream ciphers, and codes

A stream cipher is (typically) an XOR operation that encrypts and decrypts one bit or one byte at a time.

- In other words, blocks of plaintext, key and ciphertext are one-bit long.



Block ciphers, stream ciphers, and codes

In contrast, codes work on words of varying length.

- Translation given by a code-book.

Word	Code
...	...
`The`	`1701`
`secret`	`5603`
`mischiefs`	`4008`
`that`	`3790`
`I`	`2879`
`set`	`0524`
...	...

```
2879 6605 1702 9853 0001 0970 3190 8817 1320 0000 = I do the wrong, and first begin to brawl.
1701 5603 4008 3790 2879 0524 7946                = The secret mischiefs that I set abroach
2879 2870 6699 1702 3982 5550 8102 7354 0000      = I lay unto the grievous charge of others.
```

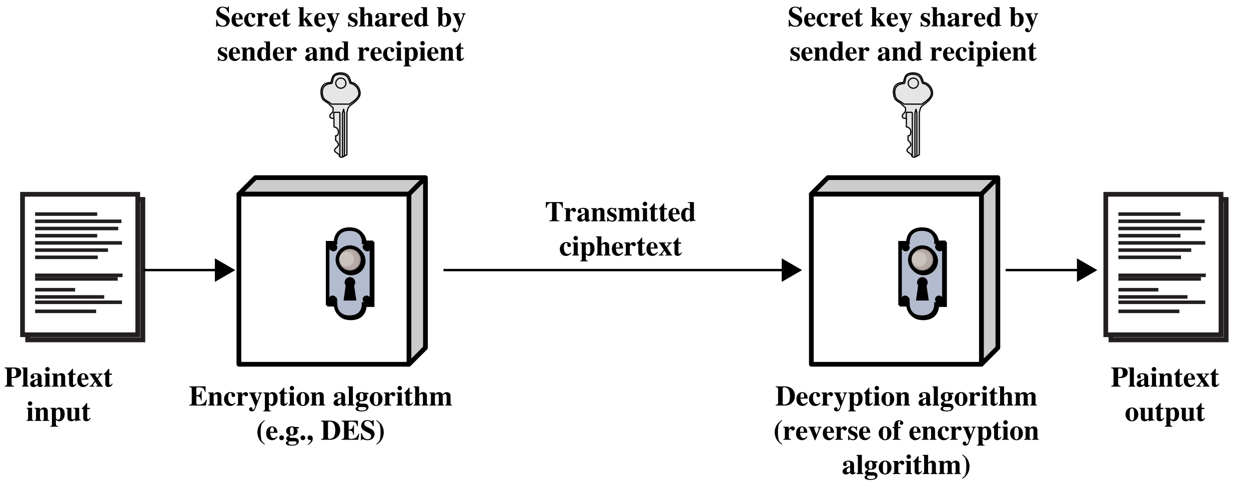
(Richard III, Act I, Scene 3)

- In general: a string of symbols stands for a complete message.
  - Example: “OCELOT" is ciphertext for “TURN LEFT 90 DEGREES" and “LOLLIPOP" is ciphertext for “TURN RIGHT 90 DEGREES".
- **Problems**:
  - if there’s no entry for “FIREWALL", then you can’t say it!
  - Security is “pushed” to the code-book, which needs to be protected.

Table of contents I

Symmetric key encryption (symmetric cipher model)

- An encryption scheme $\{E_e \mid e \in \mathcal{K}\}$ and $\{D_d \mid d \in \mathcal{K}\}$ is symmetric-key if for each associated pair (e, d) it is computationally "easy" to determine d knowing only e and to determine e from d. In practice $e = d$.
  - Also known as: secret-key, single-key, one-key, shared-key, conventional encryption.
  - Sender and recipient share a common key.
  - All classical encryption algorithms are symmetric-key (it was only type of encryption prior to invention of public-key crypto in 1970's).
  - Most widely used.



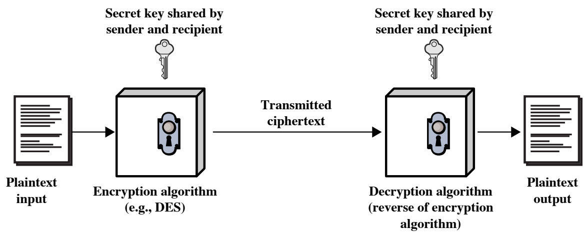
2 requirements for secure use of symmetric encryption

1. A strong encryption algorithm.

- At a minimum: attacker who knows algorithm and has access to one or more ciphertexts should be unable to decipher ciphertext or figure out key.
- Stronger: attacker should be unable to decrypt ciphertext or discover key even if he/she is in possession of a number of ciphertexts together with plaintext that produced each ciphertext.

2. Sender and receiver must obtain copies of secret key in a secure fashion (e.g., a secure channel) and must keep key secure.

- If someone can discover the key and knows the algorithm, all communication using this key is readable.

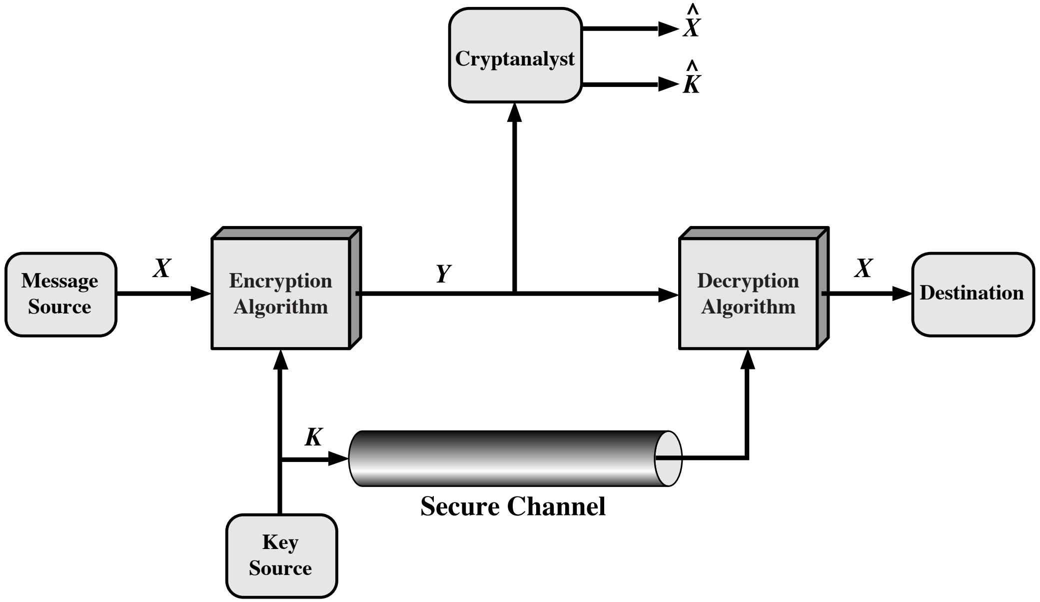


Keep only the key secret

**We do not need to keep the algorithm secret;
we need to keep only the key secret.**

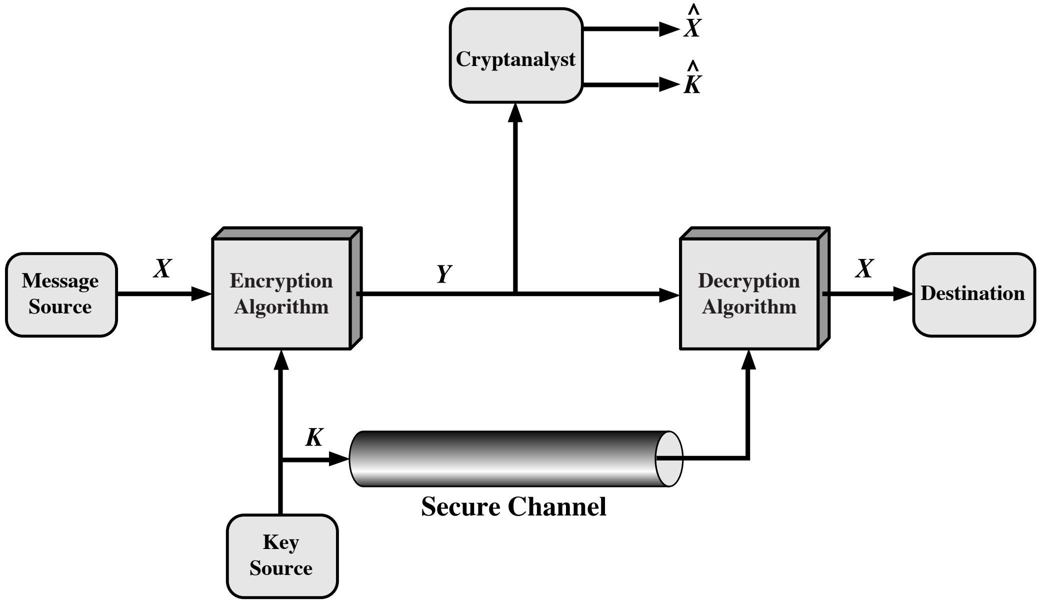
- We assume that is impractical to decrypt a message on basis of ciphertext *plus* knowledge of encryption/decryption algorithm.
- This makes symmetric encryption feasible for widespread use:
  - Manufacturers can and have developed low-cost chip implementations of data encryption algorithms.
  - Chips widely available and incorporated into a number of products.

Detailed model of symmetric cryptosystem



- A source produces a message in plaintext: $X = [X_1, X_2, \ldots, X_i]$. The i elements of X are letters in some finite alphabet.
  - Traditionally: alphabet consisted of the 26 capital letters.
  - Nowadays: binary alphabet $\{0, 1\}$ typically used.
- An encryption key of the form $K = [K_1, K_2, \ldots, K_j]$ is generated.
  - If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel.
  - Alternatively, a third party could generate the key and securely deliver it to both source and destination.

Detailed model of symmetric cryptosystem



- Encryption algo forms ciphertext $Y = E(K, X) = [Y_1, Y_2, \ldots, Y_n]$.
- The intended receiver, in possession of the key K, is able to invert the transformation: $X = D(K, Y)$.
- Attacker
  - knows the encryption (E) and decryption (D) algorithms,
  - observing Y but not having access to K or X, may attempt to recover X or K or both X and K, by generating $\hat{X}$ and/or $\hat{K}$.