

Cryptography and Cryptanalysis

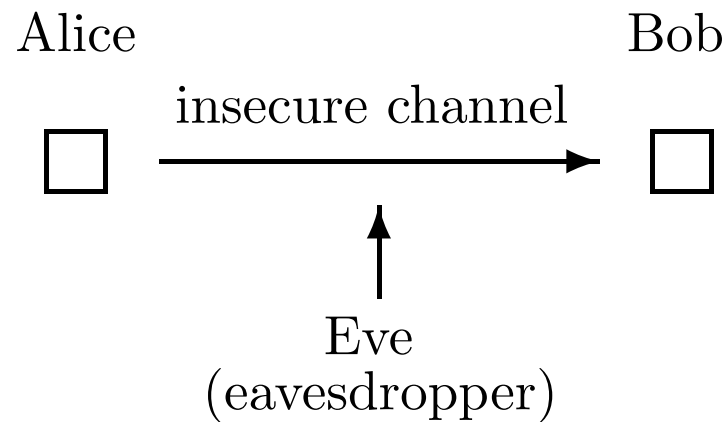
Feryâl Alayont

University of Arizona

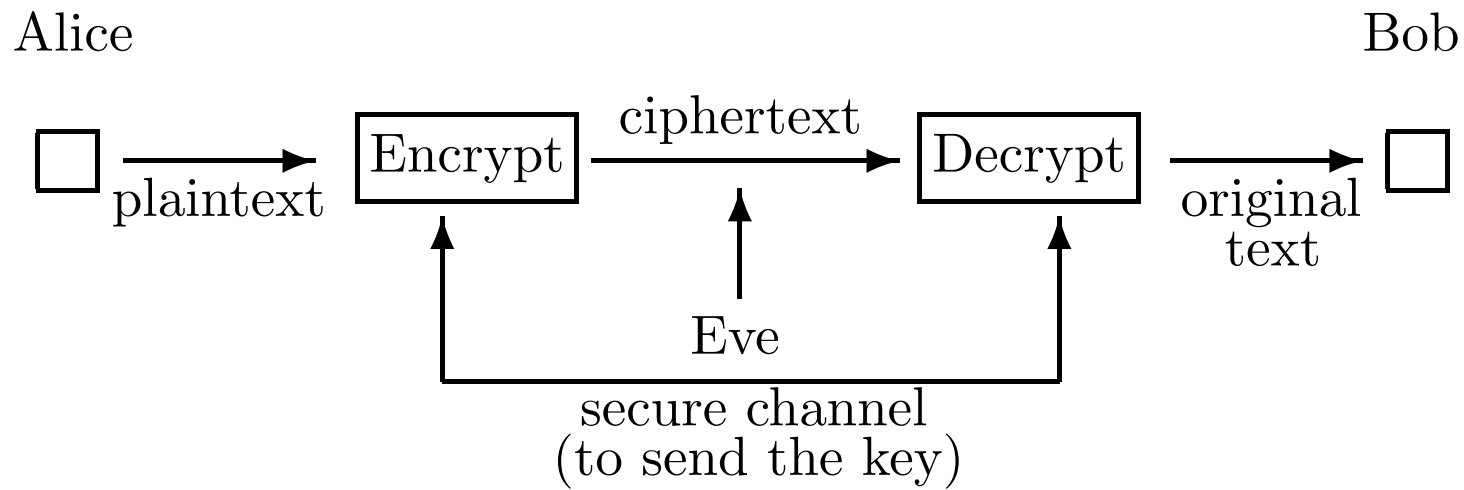
December 9, 2003

Cryptography: derived from the Greek words *kryptos*, meaning **hidden**, and *graphos*, meaning **writing**.

Cryptography is the art of “secret writing”; its intend is to provide secure communication over insecure channels.



A cryptosystem or cipher is a procedure to render messages unintelligible except to the authorized or intended recipient.



More precisely:

A cryptosystem consists of two sets, a set of possible plaintexts and a set of possible ciphertexts, and an invertible function e_k , where k is the key, from the set of plaintexts to the ciphertexts. The encryption of a plaintext m is the ciphertext $e_k(m)$ and the decryption function is e_k^{-1} :

$$e_k^{-1}(\text{ciphertext}) = e_k^{-1}(e_k(m)) = m = \text{plaintext}$$

Example: The Caesar cipher:

To encrypt a message, each letter in the message is moved forward by 3. We get the following map for letter substitution:

$$a \rightarrow D \quad b \rightarrow E \quad c \rightarrow F \quad \dots x \rightarrow A \quad y \rightarrow B \quad z \rightarrow C$$

The encryption of the plaintext

attack on tuesday

is the ciphertext

DWWDEN RQ WXHVGDB

Cryptanalysis is the art of breaking into secure communications. More precisely, a cryptanalyst tries to obtain the plaintext or the decryption function in a cryptosystem by eavesdropping into the insecure channel.

Kerckhoffs's principle: The encryption and the decryption procedure should be viewed as public knowledge, with the only secret being the key.

There are various levels of attacks on a cryptosystem.

- Ciphertext only: The cryptanalyst tries to determine the plaintext or the decryption function from the knowledge of a piece of ciphertext.
- Known plaintext: The cryptanalyst possesses both the plaintext and the ciphertext and tries to determine the decryption function.
- Chosen plaintext: The cryptanalyst can choose some number of plaintexts and see the corresponding ciphertexts.

A cryptosystem should be at least resistant to ciphertext only attacks. And actually the current standard is that a cryptosystem should be resistant to chosen plaintext attacks.

Example: Trying to improve the Caesar cipher: The shift cipher
Both sides agree in advance upon a key k , a number from 1 to 25
telling how far to shift. To encrypt a message, each letter is moved
forward k times. To decrypt, move each letter backward k times.

An adversary who had intercepted a message encrypted by a shift
cipher would have to shift the whole message by all the possible
keys, 25 of them, to find the actual key.

A smarter adversary on the other hand will decrypt only a four-five letter piece of the whole message to see which decryption makes sense in English and find the key using that piece only.

Conclusion: Even though there are 25 possible keys, no matter how long the message is it is very easy to break the shift cipher.

A bit of modular arithmetic

We let $x \bmod m$ denote the positive remainder of the division-by-remainder of x by m . For example

$$10 \bmod 7 = 3$$

$$4 \bmod 7 = 4$$

$$-4 \bmod 7 = 3$$

$$4 - 8 \bmod 7 = 3$$

$$2 \cdot 4 \bmod 7 = 1$$

$$1/4 \bmod 7 = 2$$

Using modular arithmetic we can describe the shift cipher function easily. To each letter in the alphabet, assign their corresponding place in the alphabet:

$$a \rightarrow 0 \quad b \rightarrow 1 \quad \dots \quad z \rightarrow 25$$

Then the shift cipher with key k corresponds to the function

$$e_k(x) = x + k \pmod{26}$$

For example shifting the letter y 3 times gives b . Numberwise y corresponds to 24 and the encryption mathematically expressed is

$$24 + 3 = 27 = 1 \pmod{26}$$

Since b corresponds to 1, the encryption of y is b .

Example: Try to improve the shift cipher: The affine cipher
For a pair (u, v) of integers from 0 to 25, the affine cipher $e_{(u,v)}$ is defined as

$$e_{(u,v)}(x) = u \cdot x + v \pmod{26}$$

The shift cipher is the special case of affine cipher with $u = 1$.

For example, if $u = 3$ and $v = 2$, the letter a is encrypted as

$$e_{(3,2)}(0) = 3 \cdot 0 + 2 = 2 \pmod{26}$$

which corresponds to c and the letter b is encrypted as

$$e_{(3,2)}(1) = 3 \cdot 1 + 2 = 5 \pmod{26}$$

which corresponds to f .

The key space with the affine cipher is 311 (not 25^2 since some of the pairs are unusable). So we expect the affine cipher to be stronger against attacks, yet obviously not very strong since it would not take much time to try all possible keys by a computer program.

The weakness of the affine cipher is not that it has a relatively small key space but that it does not hide the characteristics of the English language. Since each letter is encrypted in the same way regardless of their position in the message, we can guess which letter is the encryption of which letter by using the distribution of letters in the English language.

Letter	Probability	Letter	Probability
E	0.127	T	0.091
A	0.082	O	0.075
I	0.070	N	0.067
...

Given ciphertext

JOHE MOOH

we count the appearances of each letter and see that O is the most frequent and H is the second. Guessing that O may be the encryption of E, the most common letter in English, and H is the encryption of T, the second common letter, we get the equations

$$u \cdot 4 + v = 14 \pmod{26}$$

$$u \cdot 19 + v = 7 \pmod{26}$$

Solving these equations mod 26 gives

$$u = 3 \quad v = 2$$

Check:

$$3 \cdot 4 + 2 = 14 \pmod{26}$$

$$3 \cdot 19 + 2 = 59 = 7 \pmod{26}$$

The decryption of the message is

lets meet

Conclusion: Even though it has a considerably larger key space than the shift cipher, the affine cipher is still not secure since it does not hide the characteristics of the language.

Example: Cryptograms

The alphabet is mixed-up using a particular formula and messages are encrypted using this particular formula for each letter. The key space is huge: we can have

$$26!=403,291,461,126,605,635,584,000,000$$

of possible permutations of the alphabet.

However, since each letter is encrypted the same way, we can again decrypt the message using the statistical features of English.

Example: A perfectly secure cipher: One-time pad (Vernam cipher)

Plaintext

$$m = (m_1, m_2, \dots, m_n)$$

Choose a key consisting of n random characters:

$$k = (k_1, k_2, \dots, k_n)$$

Then the encryption function is

$$e_k(m) = (m_1 + k_1 \pmod{26}, m_2 + k_2 \pmod{26}, \dots, m_n + k_n \pmod{26})$$

Since the key consists of random characters, someone intercepting the ciphertext will not be able to obtain any information about the plaintext m . So one-time pad is a perfectly secure cryptosystem, as long as each key is used once. But it is difficult to distribute one key per encryption.

Example: The Vigenere cipher

Divide the message into small pieces on which one-time pad is applied. If the key is $k = (k_1, \dots, k_n)$ and the message is $m = (m_1, \dots, m_N)$ where the number of characters in the message is r times the number of characters in the key, the encryption function is

$$e_k(m) = m + \overset{r \text{ times}}{(k, \dots, k)} \pmod{26}$$

To break the Vigenere cipher we first guess the key, either by the method of Kasiski or the Friedman attack.

If the key is chosen from a dictionary, then the Vigenere cipher may be broken by brute-force by trying all the words from the dictionary as the possible key of a given length.

If the key is chosen to be not special, the Vigenere cipher seems to be somewhat secure. However, the Friedman attack guesses the key by taking the slices of the ciphertext which are encrypted by shifting the same amount.

Shannon's **Confusion and diffusion principle**

- A cipher should hide local parts in a language from the attacker.
- A cipher should mix around the different parts of the plaintext so that nothing is left in its original place.

Example: DES (Data Encryption Standard) and triple DES

A DES encryption uses a 56-bit key (plus 8 more bits for error checking) and consists of 16 rounds (repetitions) of applying a simpler process (called Feistel networks) to the message in halves. It is computationally secure, meaning it takes a long time to crack the cipher. With the advance of technology, now the standard is triple DES which is a three times application of DES. It seems to be secure for the moment.

References:

Gilles Brassard, *Modern Cryptology*, Lecture Notes in Computer Science, No. 325, 1988.

Paul B. Garrett, *Cryptology and Number Theory*, Course notes, 1999.

Douglas S. Stinton, *Cryptography: Theory and Practice*, 2002.

D. R. Hankerson, et. al, *Coding Theory and Cryptography: The Essentials*, 2000.