Information Theory
Degree in Data Science and Engineering
Lesson 7: Cryptography

Jordi Quer, Josep Vidal

Mathematics Department, Signal Theory and Communications Department
{jordi.quer, josep.vidal}@upc.edu

2019/20 - Q1

Cryptography and cryptanalysis

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure channels so that it cannot be read by anyone except the intended recipient.

Cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

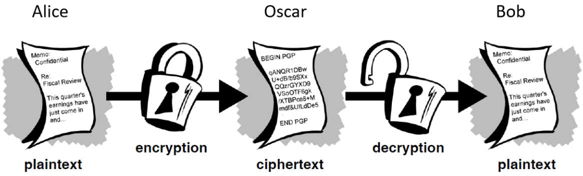
Cryptology embraces both cryptography and cryptanalysis.

Eavesdropping

The purpose of *cryptography* is to enable two people, Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, cannot understand what is being said. The information generated by Alice may be text, numerical data or anything at all.

To that end, Alice encrypts the plaintext, using a key, and sends the resulting cyphertext over the channel.

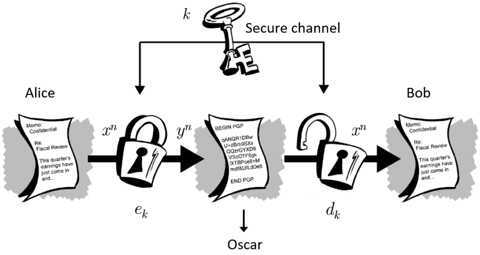
Oscar, upon seeing the text by eavesdropping cannot determine the plain text; but Bob, who knows the encryption key, can decrypt the cyphetext and reconstruct the plaintext.



Definition of a cryptosystem

A cryptosystem is defined as a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ with the following conditions:

1. $\mathcal{P}$ is finite set of possible plaintexts $x^n = x_1 x_2 \dots x_n$
2. $\mathcal{C}$ is finite set of possible cyphertexts $y^n = y_1 y_2 \dots y_n$
3. $\mathcal{K}$, the keyspace, is a finite set of possible keys k
4. For each $k \in \mathcal{K}$ there is an encryption rule $e_k \in \mathcal{E} : \mathcal{P} \to \mathcal{C}$ and a corresponding decryption rule $d_k \in \mathcal{D} : \mathcal{C} \to \mathcal{P}$, such that $d_k(e_k(x^n)) = x^n$ for every possible plaintext $x^n \in \mathcal{P}$.



Definition of a cryptosystem

A cryptosystem of practical use should meet these three properties:

- The encryption function e_k must be an injective function so that decryption is unambiguous:

$$x_i \neq x_j \quad \Rightarrow \quad e_k(x_i) \neq e_k(x_j) \ \forall i, j$$

- The eavesdropper, upon seeing the ciphertext y^n should be unable to determine the key k that was used, or the plaintext x^n.
- Encryption function e_k and decryption function d_k should be efficiently computable.

The second property is defining the idea of *security*.

Check this *link* for codes and ciphers in history.

Cryptoanalysis

The general assumption is that the opponent, Oscar, knows the cryptosystem being used (which is a worst situation for Alice and Bob), and is interested in decripting the message y^n or more generally getting the key k. We want to assure security in this case.

The most common types of attack models are:

- **Ciphertext-only attack**. Oscar possesses a string of ciphertext, y^n.
- **Known plain text attack**. Oscar possesses a string of plain text x^n and the corresponding cyphertext, y^n.
- **Chosen plaintext attack**. Oscar has temporary access to the encryption machine, choses x^n and constructs y^n.
- **Chosen ciphertext attack**. Oscar has temporary access to the decryption machine, choses y^n and constructs x^n.

In the sequel, we consider the ciphertext-only attack, which is the weakest one.

Cryptosystems: shift cipher

Let us describe some cryptosystems where both Alice and Bob have previously agreed on a key k.

We shall assume that $\mathbb{Z}_m$ is a *field* defined in the set $\{0, ..., m-1\}$ equiped with the addition and multiplication operations, both modulo m. Examples of application will encrypt text by assigning $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$, and hence $\mathbb{Z}_{26}$.

Cryptosystem (The Shift Cipher)

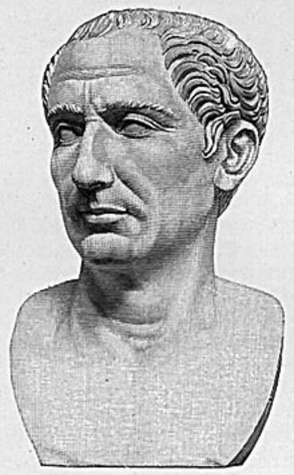
Let m be a positive integer. $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$. For $0 \leq k \leq m$, define

$$e_k(x) = (x + k) \textit{ mod}\, m \qquad d_k(y) = (y - k) \textit{ mod}\, m$$

with $(x, y) \in \mathbb{Z}_m$.

Cryptosystems: shift cipher

"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the other.", Gaius Suetonius, in *Life of Julius Caesar* 56



Cryptosystems: shift cipher

Example. Take $m = 26$, the key is $k = 11$, and the plain text is

```
wewillmeetatmidnight
```

To apply the rule, first convert the text to integers:

$$22\ 4\ 22\ 8\ 11\ 11\ 12\ 4\ 4\ 19\ 0\ 19\ 12\ 8\ 3\ 13\ 8\ 6\ 7\ 19$$

and we add 11 to each value reducing the sum mod 26:

$$7\ 15\ 7\ 19\ 22\ 22\ 23\ 15\ 15\ 4\ 11\ 4\ 23\ 19\ 14\ 24\ 19\ 17\ 18\ 4$$

By converting the sequence of integers to alphabetic characters, the ciphertext is:

```
HPHTWWXPPELEXTOYTRSE
```

Cryptanalysis. Shift cipher is not secure, since it can be cryptanalyzed by *exhaustive key search*: it is easy to try every possible decryption rule $d_0, \ldots, d_{m-1}$ until a meaningful plaintext is obtained.

Cryptosystems: substitution cipher

Cryptosystem (The Substitution Cipher)

Let m be a positive integer. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$. $\mathcal{K}$ consists of all possible permutations of the m symbols $\{0, 1, \dots m\}$. For each permutation $\pi \in \mathcal{K}$, define

$$e_\pi(x) = \pi(x) \qquad d_\pi(y) = \pi^{-1}(y),$$

where π^{-1} is the inverse permutation to π.

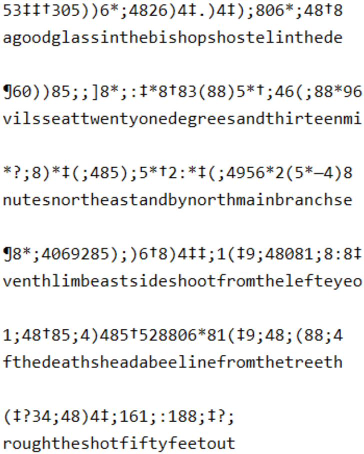
Example. Encryption and decryption are permutations of alphabetic characters. An example of random permutation π for all the alphabet:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

thus $e_\pi(\mathtt{a}) = \mathtt{X}$, $e_\pi(\mathtt{b}) = \mathtt{N}$, etc. The decryption rule is trivial.

Cryptosystems: substitution cipher



```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
agoodglassinthebishopshostelinthede

¶60))85;;]8*;:‡*8†83(88)5*†;46(;88*96
vilsseattwentyonedegreesandthirteenmi

*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8
nutesnortheastandbynorthmainbranchse

¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
venthlimbeastsideshootfromthelefteyeo

1;48†85;4)485†528806*81(‡9;48;(88;4
fthedeathsheadabeelinefromthetreeth

(‡?34;48)4‡;161;:188;‡?;
roughtheshotfiftyfeetout
```

Cryptosystems: substitution cipher

Cryptanalysis. A key consist of a permutation of the m symbols, and the number of permutations is $m!$ For $m = 26$, $m! = 4.0 \times 10^{26}$, and exhaustive search is infeasible for a computer. However, the substitution cipher can be cryptanalized using a smarter method.

Many cryptanalysis techniques use the statistical properties of the language of the plaintext. Let us illustrate it with an example: according to the relative frequencies of the 26 letters in English, they can be grouped as

1. e, having probability about 0.120
2. `t,a,o,i,n,s,h,r`, having probability between 0.06 and 0.09
3. `d,l`, each having probability around 0.04
4. `c,u,m,w,f,g,y,p,b`, having probability between 0.015 and 0.028
5. `v,k,j,x,q,z`, each having probability less than 0.01

Cryptosystems: substitution cipher

Consider Oscar has received the following ciphertext:

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

and wants to decipher it. The frequency analysis of this ciphertext is:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	0	1	15	13	7	11	1	4	5	11	1	0	16

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	9	0	1	4	10	3	2	5	5	8	6	10	20

- Single letter analysis. Since Z occurs more, we conjecture $d_k(\mathtt{Z}) = \mathtt{e}$. The characters C,D,F,J,M,R,Y occur at least 10 times, so they could be encriptions of t,a,o,i,n,s,h,r, but the frequencies are too similar to conclude a correspondence.

Cryptosystems: substitution cipher

- Digram analysis. Let us look at digrams, starting with those of the form `-Z` and `Z-`, since we conjecture $d_k(\mathtt{Z}) = \mathtt{e}$. Most common digrams are `DZ` and `ZW` (4 times); `NZ` and `NU` (3 times); `RZ,HZ,XZ,FZ,ZR`, `ZV,ZC,ZD` and `ZJ` (twice each).

Since `ZW` occurs 4 times and `WZ` not at all, and `W` occurs less often than many other characters, we guess $d_k(\mathtt{W}) = \mathtt{d}$.

Since `DZ` occurs 4 times and `ZD` occurs twice, we can conjecture $d_k(\mathtt{D}) \in \{\mathtt{r},\mathtt{s},\mathtt{t}\}$ but it is not clear which is the correct one.

- Trigram analysis. Taking the assumptions $d_k(\mathtt{Z}) = \mathtt{e}$ and $d_k(\mathtt{W}) = \mathtt{d}$, we notice that `ZRW` occurs near the beginning of the ciphertext, and `RW` occurs again later on. Since `R` occurs frequently and nd is a common digram in English, we can guess $d_k(\mathtt{R}) = \mathtt{n}$ as the most likely possibility.

Cryptosystems: substitution cipher

At this point we have the following deciphering:

```
------end---------e----ned---e------------
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
--------e----e---------n--d---en----e----e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
-e---n------n------ed---e---e--ne-nd-e-e--
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
-ed-----n-----------e----ed-------d---e--n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Next, turn to single letter analysis trying $d_k(\mathtt{N}) = \mathtt{h}$, since NZ is a common digram and ZN is not, if this is right, the segment of plain text ne-ndhe suggests $d_k(\mathtt{C}) = \mathtt{a}$.

Cryptosystems: substitution cipher

Now consider M, the second most common ciphertext character. The ciphertext RNM, believed to decrypt to nh-, suggests that h- begins a word, so M is most likely a vowel. Since we have already have conjectures for a and e, we expect that $d_k(\mathtt{M}) \in \{\mathtt{i,o,u}\}$. Since ai is a much more likely digram than ao, the digram CM suggests that we try $d_k(\mathtt{M}) = \mathtt{i}$ first. Then we have:

```
-----iend-----a-i-e-a-inedhi-e------a---i-
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
h-----i-ea-i-e-a---a-i-nhad-a-en--a-e-hi-e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
he-a-n-----in-i----ed---e---e-ineandhe-e--
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
-ed-a--inhi--hai--a-e-i--ed-----a-d--he--n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptosystems: substitution cipher

Let us try to determine which letter is the encryption of `o`: among the most common ciphertext is `D,F,J,Y`, `Y` seems the most likely possibility. Otherwise, we would get strings of three vowels (which are very unlikely). Hence $d_k(\mathtt{Y}) = \mathtt{o}$.

The three most frequent remaining ciphertext letters are `D,F,J` which we conjecture could decript to `r,s,t` in some order. Two occurrences of the trigram `NMD` suggest $d_k(\mathtt{D}) = \mathtt{s}$, giving the trigram `his` in plaintext. The segment `HNCMF` could be an encryption of `chair`, which would give $d_k(\mathtt{F}) = \mathtt{r}$ and $d_k(\mathtt{H}) = \mathtt{c}$, and then by elimination $d_k(\mathtt{J}) = \mathtt{t}$.

Now we have:

Cryptosystems: substitution cipher

```
o-r-riend-ro--arise-a-inedhise--t---ass-it

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

hs-r-riseasi-e-a-orationhadta-en--ace-hi-e

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he-asnt-oo-in-i-o-redso-e-ore-ineandhesett

NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-ac-inhischair-aceti-ted--to-ardsthes-n

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

From which it is easy to determine the plaintext and the key. The complete decription is (included spaces for ease of reading):

```
our friend from Paris examined his empty glass with
surprise as if evaporation had taken place while he
wasn't looking. I poured some more wine and he settled
back in his chair, face tilted up towards the sun.
```

Cryptosystems: affine cipher

Cryptosystem (The Affine Cipher)

Let m be a positive integer. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$ and let

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m : \textit{gcd}(a, m) = 1\}$$

For $k = (a, b) \in \mathcal{K}$, define

$$e_k(x) = (ax + b) \textit{ mod } m \qquad d_k(y) = a^{-1}(y - b) \textit{ mod } m$$

with $(x, y) \in \mathbb{Z}_m$.

Note that both the shift cipher and the affine cipher are special cases of the substitution cipher.

For decryption to be possible, it is necessary to find when an affine function is injective. In other words, we want the congruence $ax + b \equiv y \pmod{m}$ to have a unique solution for x. Since $y - b$ also varies over $\mathbb{Z}_m$, it suffices to study the congruence $ax \equiv y \pmod{m}$.

Cryptosystems: affine cipher

Theorem (7.1)

The congruence $ax \equiv y \pmod{m}$ has a unique solution $x \in \mathbb{Z}_m$ for every $y \in \mathbb{Z}_m$ if and only if gcd$(a, m) = 1$.

Proof. Suppose that $\gcd(a, m) = d > 1$. Then, $ax \equiv 0 \pmod{m}$ has at least two solutions, $x = 0$ and $x = m/d$. Then $e(x) = (ax + b) \bmod m$ is not an injective function and cannot be an encrypter.

Assume now that $\gcd(a, m) = 1$. Take x_1 and x_2 such that

$$ax_1 \equiv ax_2 \pmod{m}$$

Then $a(x_1 - x_2) \equiv 0 \pmod{m}$. From the fundamental property of integer division: if $\gcd(a, b) = 1$ and a divides bc, then a divides c. Therefore, if m divides $a(x_1 - x_2)$, since $\gcd(a, m) = 1$, it follows that m divides $(x_1 - x_2)$ and hence $x_1 \equiv x_2 \bmod m$. Since $x \in \{0, ..., m - 1\}$, then $x_1 = x_2$. □

Cryptosystems: affine cipher

How to prove the decryption rule? Let us consider the congruence:

$$y \equiv ax + b \pmod{m}$$

which is equivalent to $ax \equiv y - b \pmod{m}$. Since $\gcd(a, m) = 1$, a has a single inverse modulo m, and

$$a^{-1}(ax) \equiv a^{-1}(y - b) \pmod{m}$$

By associativity we have $a^{-1}(ax) \equiv (a^{-1}a)x \equiv x \pmod{m}$ and consequently the decripton function is

$$d_k(y) = a^{-1}(y - b) \bmod m$$

How to compute inverses in $\mathbb{Z}_m$? Using the *Euclidean algorithm* (see annex) for multiplicative inverses, that is, solving the diophantic equation $a\alpha + m\beta = 1$ for $\alpha, \beta \in \mathbb{Z}$ to get the inverse of a in α.

Cryptosystems: affine cipher

Cryptanalysis. Let us evaluate the number of possible values of a and b. The number of integers in $\mathbb{Z}_m$ that are relative prime to m is denoted by the Euler function $\phi(m)$.

Theorem (7.2)

Assume the factorization

$$m = \prod_{i=1}^{n} p_i^{e_i}$$

where p_i are distinct prime numbers and $e_i > 0,\ 1 \leq i \leq n$. Then

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1}\right)$$

Since $b \in \mathbb{Z}_m$, the total number of keys is $m \cdot \phi(m)$. Therefore, for $m = 26$, the number of keys is $m \cdot \phi(m) = 26 \times 12 = 312$. This is a very small number!

Let us see a procedure to decrypt the affine cipher.

Cryptosystems: affine cipher

Consider Oscar has received the following ciphertext:

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSH
VUFEDKAPRKDLYEVLRHHRH
```

and wants to decipher it by guessing a and b.

Single letter analysis. The most frequent ciphertext characters are: `R` (8 times), `D` (7 times), `E,H,K` (5 times each) and `F,S,V` (4 times each).

Let us proceed by formulating hypotheses, starting with the most likely:

Cryptosystems: affine cipher

- `R` is the encryption of `e` and `D` is the encryption of `t`. That is, $e_k(4) = 17$ and $e_k(19) = 3$. We get two linear equations (recalling that $e_k(x) = ax + b$) with the unknowns a and b, for which $a = 6$, $b = 19$ (in $\mathbb{Z}_{26}$). But this is an illegal key since $\gcd(a, 26) = 2 > 1$. The hypotheses is incorrect.
- `R` is the encryption of `e` and `E` is the encryption of `t`. $a = 8$, impossible.
- `R` is the encryption of `e` and `K` is the encryption of `t`. $a = 3, b = 5$, which is a legal key. We have to check if the decrypted text is meaningful. Now $3^{-1} \equiv 9 \pmod{26}$, $3^{-1} \times 5 \equiv 19 \pmod{26}$.

The cyphertext decripts to yield:

```
algorithmsarequitegeneraldefinitions
ofarithmeticprocesses
```

Cryptosystems: Vigenère cipher

Cryptosystem (The Vigenère Cipher)

Let m and r be positive integers. Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^r$. For a key $k^r = k_1 k_2 \ldots k_r$, we define

$$e_{k^r}(x_1, x_2, \ldots, x_r) = (x_1 + k_1, x_2 + k_2, \ldots, x_r + k_r)$$

and

$$d_{k^r}(y_1, y_2, \ldots, y_r) = (y_1 - k_1, y_2 - k_2, \ldots, y_r - k_r),$$

where all operations are performed modulo m.

Unlike the previous cases, this is a polyalphabetic cryptosystem. It is attributed to *Blaise de Vigenère*, French diplomat from XVI century.

Cryptanalysis. The number of possible keywords of length r is m^r. For $m = 26$ and $r = 10$, $m^r = 1.4 \times 10^{14}$. This is a large number of keys, but an exhaustive search is still feasible for a computer.

Cryptosystems: permutation cipher

Instead of changing each character in the plaintext by another, we can alter the position of the characters by using a permutation.

Cryptosystem (The Permutation Cipher)

Let m *and* r *be positive integers. Let* $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_m)^r$ *and let* $\mathcal{K}$ *consist of all permutations of* $\{1, \ldots, m\}$*. For a key* π*, we define*

$$e_\pi(x_1, \ldots, x_r) = (x_{\pi(1)}, \ldots, x_{\pi(r)})$$

and

$$d_\pi(y_1, \ldots, y_r) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(r)}),$$

where π^{-1} *is the inverse permutation to* π*.*

Security of a cryptosystem

The most useful criteria to evaluate the security of a cryptosystem are:

- Computational security. The computational effort required to break a cryptosystem: the best algorithm for breaking requires N operations, with N very large. No known practical cryptosystem can be proved to be secure under this definition.
- Provable security. By reduction to another problem, for example, "a cryptosystem is secure if a given integer n cannot be factored".
- Unconditional security. The system cannot be broken even with infinite computational resources.

When discussing the security of a cryptosystem, it is important to specify the type of attack that is being considered. We have seen that neither the Shift Cipher, the Substitution Cipher nor the Vigenère Cipher are computationally secure against ciphertext-only attack.

A probabilistic model for secrecy

Let us develop a theory of cryptosytems that are unconditionally secure against ciphertext-only attacks based on a probabilistic model: assume that a cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined and a particular key $k \in \mathcal{K}$ is used only for one encription. Then,

- $\Pr(X = x) = p(x)$ is the probability of observing the plaintext x.
- $\Pr(K = k) = p(k)$ is the probability of key k being used.
- Assume X and K are independent random variables.
- The set of possible ciphertexts if k is used: $\mathcal{C}(k) = \{e_k(x) : x \in \mathcal{P}\}$

Since the ciphered text y is also random, we can write

$$p(y) = \Pr(Y = y) = \sum_{\{k : y \in \mathcal{C}(k)\}} p(y|k)p(k) = \sum_{\{k : y \in \mathcal{C}(k)\}} \Pr(X = d_k(y))p(k)$$

$$p(y|x) = \Pr(Y = y|X = x) = \sum_{\{k : y \in \mathcal{C}(k)\}} p(y|x, k)p(k) = \sum_{\{k : x = d_k(y)\}} p(k)$$

A probabilistic model for secrecy

By using Bayes' theorem, it is straightforward to compute $p(x|y)$. Now, we can define perfect secrecy meaning that Oscar can obtain no information about the plaintext x by observing the ciphertext y:

Definition

A cryptosystem has *perfect secrecy* if $p(x|y) = p(x)$ for all $x \in \mathcal{P}, y \in \mathcal{C}$.

We can now formally prove that the *Shift Cipher* provides perfect secrecy: it is unbreakable provided that a new random key is used to encrypt every plaintext character.

Perfect secrecy of the shift cipher

Theorem (7.3)

Assume m keys are used with equal probability. Then, for any plaintext probability distribution, the Shift Cipher has perfect secrecy.

Proof. Recall that $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$ and the encription rule $e_k(x) = (x + k) \bmod m$, for $0 \leq k \leq m$. The probability distribution on $\mathcal{C}$ is:

$$p(y) = \sum_{k \in \mathbb{Z}_m} \Pr(X = d_k(y))p(k) = \sum_{k \in \mathbb{Z}_m} \frac{1}{m} \Pr(X = (y{-}k)\mathrm{mod} m) = \frac{1}{m} \sum_{k \in \mathbb{Z}_m} p(x)$$

where in the last equality we use that, for a fixed value of y, the values $x = (y - k) \bmod m$ are permutations of $\mathbb{Z}_m$. By changing k all possible values are covered, last summation is 1 and $p(y) = \frac{1}{m}$.

Since for a given pair x, y there is a unique key k such that $e_k(x) = y$, then $p(y|x) = \Pr(K = (y - x) \bmod m) = \frac{1}{m}$. Now we can use these results in Bayes' theorem to conclude

$$p(x|y) = \frac{p(x)p(y|x)}{p(y)} = p(x). \qquad \square$$

Shannon's theorem

A general characterization of what perfect secrecy entails is originally due to Shannon.

Theorem (C. Shannon, 1950)

Assume that a cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *where* $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. *Then, the cryptosystem provides perfect secrecy if and only if every key is used with equal probability* $1/|\mathcal{K}|$, *and for every* $x \in \mathcal{P}$ *and every* $y \in \mathcal{C}$, *there is a unique key* k *such that* $e_k(x) = y$.

Proof: Necessary condition

Suppose the system provides perfect secrecy. For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there must be a key k such that $e_k(x) = y$, so we have

$$|\mathcal{C}| = |\{e_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

Since we are assuming equality, there are not two different keys k_1 and k_2 such that $e_{k_1}(x) = e_{k_2}(x) = y$.

Shannon's theorem

Proof: Necessary condition (cont.)

Denote $n = |\mathcal{K}|$. Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$. Name the keys $k_1, k_2, ..., k_n$ such that $e_{k_i}(x_i) = y, 1 \leq i \leq n$. Using Bayes' theorem

$$p(x_i|y) = \frac{p(y|x_i)p(x_i)}{p(y)} = \frac{p(k_i)p(x_i)}{p(y)}$$

If we consider the perfect secrecy condition $p(x_i|y) = p(x_i)$, it follows that $p(k_i) = p(y)$, for $1 \leq i \leq n$, so all keys have to be used with equal probability (namely, $p(y)$), but since the number of keys is $|\mathcal{K}|$ then $p(k_i) = 1/|\mathcal{K}|$ for every $k_i \in \mathcal{K}$.

Sufficient condition

It follows straightforward from theorem 7.3. □

Cryptosystems: One-time pad

According to Shannon's theorem, one cryptosystem that provides full secrecy is the *One-time Pad cipher*:

Cryptosystem (The One-time pad Cipher)

Let m, n be positive integers. Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^n$. For $k \in (\mathbb{Z}_m)^n$, define $e_k(x)$ to be the vector sum modulo m of k and x. So, if $x^n = (x_1, \dots, x_n)$ and $k^n = (k_1, \dots, k_n)$, then

$$e_k(x^n) = (x_1 + k_1, \dots x_n + k_n) \, mod \, m$$

Decription is identical to encryption. If $y^n = (y_1, \dots, y_n)$, then

$$d_k(y^n) = (y_1 - k_1, \dots y_n - k_n) \, mod \, m$$

Cryptosystems: One-time pad

One-time pad was first described by G. Vernam in 1917. It was believed that it was unbreakable for many years, but there was no mathematical proof until Shannon's theorem. Encryption and decryption are simple, but the disadvantages are serious:

- $|\mathcal{K}| \geq |\mathcal{P}|$ means that the amount of keys must at least be as big as the amount of plaintext.
- It would be vulnerable to a known-plaintext attack, since k^n can be computed by a difference modulo m between x^n and y^n, if the key were used more than once.

This creates severe key management problems which have limited the use of one-time pad except for military and diplomatic contexts where unconditional security is of utmost importance.

Secrecy when reusing a key

The development of cryptography is associated to the need of designing cryptosystems where one key can be used to encrypt many messages of plaintext and still maintain some computational security.

For an encryption system to be secure, a necessary condition is that an exhaustive key search should be infeasible; i.e. the keyspace should be very large. However, a large keyspace is not sufficient to guarantee perfect secrecy.

"Information is only secure when it costs more to get it than it's worth."
Kevin Poulsen (hacking pioneer)

Secrecy when reusing a key

Take a cryptosystem in which the key is reused over several plaintext characters, and assume Oscar has infinite computational resources to do a ciphertext-only attack. We want to answer the question: given $y = d_k(x)$ how many keys would provide a meaninful deciphered message?

Example. Oscar obtains the ciphertext string `WNAJW`, encripted using shift cipher. There are two meaningful plaintext strings, namely `river` and `arena`, corresponding to two possible encription keys, $k = 5$ and $k = 22$. One of them is a *spurious key*.

Let us find a bound on the number of spurious keys by using our knowledge on entropy. Of course Alice and Bob are interested in this number to be large.

Secrecy when reusing a key

Define the key equivocation $H(K|C)$ as the remaining uncertainty about the key when the cyphertext is known.

Theorem (7.5)

Let $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ *be a cryptosystem. Then*

$$H(K|C) = H(K) + H(P) - H(C)$$

Proof. Observe that $H(K,P,C) = H(K,P) + H(C|K,P)$. Since the key and the plaintext determine uniquely the ciphertext, $H(C|K,P) = 0$. But the random variables K and P are independent, so

$$H(K,P,C) = H(K,P) = H(K) + H(P).$$

Similarly, since the key and the ciphertext determine the plaintext uniquely, $H(P|K,C) = 0$ and hence $H(K,P,C) = H(K,C)$.

Secrecy when reusing a key

Proof (cont.) Now we compute the key equivocation as follows:

$$H(K|C) = H(K,C) - H(C) = H(K,P,C) - H(C) = H(K) + H(P) - H(C)$$

and the result is complete. □

Now we can derive the average number of spurious keys:

Theorem (7.6)

Suppose $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ is a cryptosystem where $|\mathcal{P}| = |\mathcal{C}|$ and keys are equiprobable. Let $R_L = 1 - H(X^n)/n \log|\mathcal{P}|$ denote the redundancy of the underlying language. Then, given a string of ciphertext of length n, where n is sufficiently large, the expected number of spurious keys $\bar{s}_n$ satisfies:

$$\bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

Secrecy when reusing a key

Proof. Given y^n, define the set of keys k for which y^n is the encription of a meaningful string of plaintext:

$$k(y^n) = \{k \in \mathcal{K} : \exists x^n \text{ such that } p(x^n) > 0 \text{ and } e_k(x^n) = y^n\}$$

The average number of spurious keys is given by

$$\bar{s}_n = \sum_{y^n \in \mathcal{C}} p(y^n)\left(|k(y^n)| - 1\right) = \sum_{y^n \in \mathcal{C}} p(y^n)|k(y^n)| - 1$$

In the result of theorem 7.5, $H(K|Y^n) = H(K) + H(X^n) - H(Y^n)$ we can use the definition

$$H(X^n) = n(1 - R_L)\log|\mathcal{P}|$$

where the entropy rate may be used for reasonably large n (see chapter 3). Since $|\mathcal{P}| = |\mathcal{C}|$ and $H(Y^n) \leq n\log|\mathcal{C}|$, then

$$H(K|Y^n) \geq H(K) - nR_L\log|\mathcal{P}|.$$

Note: Remember from lesson 3 that in English $\frac{1}{n}H(X^n) \simeq 1.2$ bits/letter for $n \leq 12$.

Secrecy when reusing a key

Proof (cont.) We can relate this expression to the average number of spurious keys:

$$H(K|Y^n) = \sum_{y^n \in \mathcal{C}} p(y^n) H(K|y^n) \leq \sum_{y^n \in \mathcal{C}} p(y^n) \log |k(y^n)|$$

$$\leq \log \sum_{y^n \in \mathcal{C}} p(y^n) |k(y^n)| = \log(\bar{s}_n + 1)$$

where Jensen's inequality has been applied. Combining the two inequalities:

$$\log(\bar{s}_n + 1) \geq H(K) - nR_L \log |\mathcal{P}|$$

and taking the keys equiprobable, we obtain the result. □

How many keys do we need to have on average 9 spurious keys for a 10 characters-long message in English?

Secrecy when reusing a key

Definition (Unicity distance)

The unicity distance of a cryptosystem is the value of n, denoted by n_0, at which the expected number of spurious keys become zero.

Setting $\bar{s}_n = 0$ in the result of theorem 7.6,

$$n_0 \simeq \frac{\log |\mathcal{K}|}{R_L \log |\mathcal{P}|}$$

Note that encription after perfect source coding implies $R_L \to 0$ and $n_0 \to \infty$.

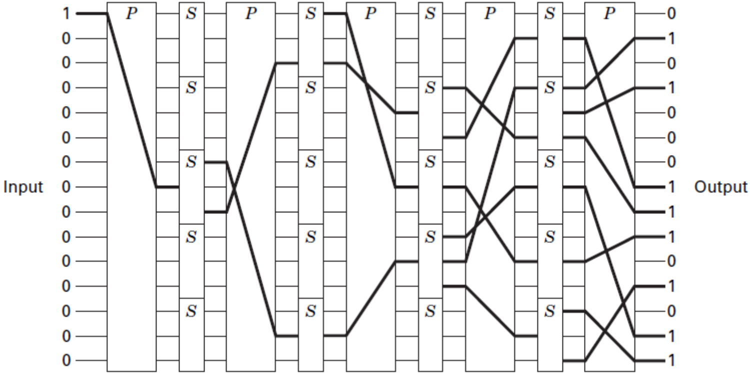
Example. Consider the Substitution Cipher, where $|\mathcal{P}| = 26$ and $|\mathcal{K}| = 26!$ From the entropy rate of English $R_L = 0.7447$, an estimate for the unicity distance is

$$n_0 \simeq 88.4/(0.6171 \times 4.7) \simeq 25$$

This suggests that, given a cyphertext string of length larger than 25, a unique decription is possible (in average). Of course, for improved secrecy, n must be below this value.

Practical symmetric cryptosystems

Shannon suggested that using a combination of substitution and permutation ciphers together could yield a cipher system more powerful than either one alone. This has become the basis for the US Data Encryption Standard (DES):

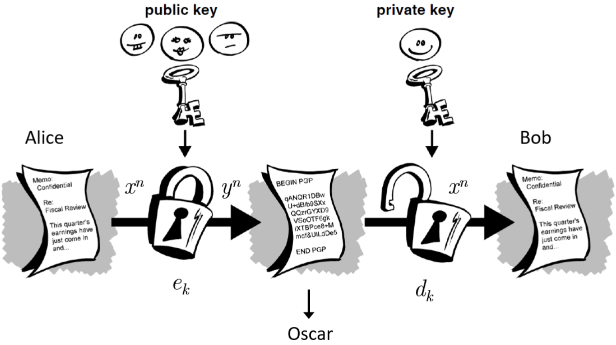


where the keys for each P and S block have to be known by Alice and Bob.

Symmetric key vs. public key systems

Symmetric key encription is fast, but it is expensive due to the difficulty of secure key distribution: a courier distributing the key must be trusted.

The problems of key distribution are solved by public key cryptography which is an asymmetric scheme that uses a pair of keys: a public key that encrypts data and a corresponding private key (kept secret) for decryption.



Symmetric key vs. public key systems

Alice can use the public key to encrypt information to Bob. Anyone that knows the public key is unable to decrypt it. Bob is the only person that can decrypt the ciphertext using the private key in the decription rule d_K.

The system is designed in such a way that it is computationally infeasible to deduce the private key from the public key. Now, Alice and Bob do not need previous security arrangements.

The idea of public-key cryptosystem was put forward by Diffie and Hellman in 1976. In 1977 Rivest, Shamir and Adleman invented the RSA cryptosystem.

RSA cryptosystem

Cryptosystem (The RSA cryptosystem)

Let $n = pq$, where p and q are relative primes and $\phi(n) = (p-1)(q-1)$. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \ (\textit{mod}\ \phi(n))\}$$

For $K = (n, p, q, a, b)$, define

$$e_K(x) = x^b \ \textit{mod}\ n \qquad\qquad d_K(y) = y^a \ \textit{mod}\ n$$

with $(x, y) \in \mathbb{Z}_n$. b is relative prime to $\phi(n)$. The values n and b are the public key. The values p, q and a are private.

Secrecy comes from the enormous computational effort required by a cryptoanalyst to factor n, although effective ways to attack it have been described.

RSA cryptosystem

Decription is possible because for any $x \in \mathbb{Z}_n$, and $ab \equiv 1 \pmod{\phi(n)}$

$$\begin{aligned}(x^b)^a &\equiv x^{t\phi(n)+1} \pmod{n} \\ &\equiv (x^{\phi(n)})^t x \pmod{n} \\ &\equiv 1^t x \pmod{n} \quad \text{By Euler's theorem, see annex 2} \\ &\equiv x \pmod{n}\end{aligned}$$

Square-and-multiply is an efficient algorithm that computes modular exponentiation $x^b \bmod n$ by decomposing b in a sum of powers of 2 and applying associativity of the modular product.

RSA cryptosystem

Example. Bob wants to receive encrypted messages, so he chooses two primes $p = 101$ and $q = 113$. Then $n = 11413$ and $\phi(n) = 100 \times 112 = 11200$. b has to be relative prime to $\phi(n)$, so Bob choses $b = 3533$. Then

$$b^{-1} \bmod 11200 = 6597$$

Bob's secret decryption exponent is $a = 6597$.

Bob publishes $n = 11413$ and $b = 3533$ in a directory. If Alice wants to encrypt the plaintext 9726 to send to Bob. She will compute:

$$9726^{3533} \bmod 11413 = 5761$$

and send the ciphertext 5761 over the channel. When Bob receives the ciphertext, he uses his secret decryption exponent to compute

$$5761^{6597} \bmod 11413 = 9726$$

Note that a cryptoanalyist would need $\phi(n)$ to recover Bob's key. This requires factoring $n = pq$ which is extremely hard for large n.

Conclusions

Certain cryptosystems are secure if the amount of ciphertext is sufficiently small. For example,

- the Shift Cipher and the Substitution Cipher are both unconditionally secure if a single element of plain text is encripted with a given key.
- the Vigenère Cipher with word length r is unconditionally secure if the key is used to encrypt only one element of plaintext (which consist of r alphabetic characters).
- for larger values of the reuse of the key, the unicity distance provides a bound on the value of n that should not be depassed.

Only public key cryptosystems are used in common practice.

Recommended bibliography: D. R. Stinson, *Cryptography. Theory and Practice*, Third edition, Chapman & Hall/CRC, 2006

Annex 1. Euclidean algorithm for modular inverse

Two numbers a and b are congruent modulo m if $(a-b)/m$ is an integer. It is denoted as $a \equiv b \pmod{m}$. Note that it implies that the remainders of a/m and b/m are equal. Let us compute the inverse $a^{-1}a \equiv 1 \pmod{m}$.

The algorithm is as follows. Let r_j be the remainder of a division:

$$\begin{aligned}
&r_1 = m - aq_1, \;\; 0 > r_1 > a \\
&r_2 = a - r_1 q_2, \;\; 0 > r_2 > r_1 \\
&r_3 = r_1 - r_2 q_2, \;\; 0 > r_3 > r_2 \\
&\quad\vdots \\
&r_j = r_{j-2} - r_{j-1} q_j, \;\; 0 > r_j > r_{j-1}
\end{aligned}$$

At this point $r_j = \text{gcd}(m, a)$. By replacing backwards the expressions we end up having $r_j = mx + ay$, where x and y are integers. Note that the algorithm can solve this diophantic equation if a solution exits. If $\text{gcd}(m, a) = 1$, then

$$1 = mx + ay \;\Leftrightarrow\; ay \equiv 1 \pmod{m}$$

If $\text{gcd}(m, a) \neq 1$, the inverse does not exist.

Annex 1. Euclidean algorithm for modular inverse

Example. Find the multiplicative inverse of 8 mod 11 using the Euclidean algorithm:

$$3 = 11 - 8 \times 1$$
$$2 = 8 - 3 \times 2$$
$$1 = 3 - 2 \times 1$$

Now reverse the process as follows:

$$\begin{aligned}
&1 = 3 - 2 \times 1\\
&1 = 3 - (8 - 3 \times 2) \times 1 = 3 \times 3 - 8\\
&1 = (11 - 8 \times 1) \times 3 - 8 = 11 \times 3 - 8 \times 4 = 11 \times 3 + 8 \times (-4)
\end{aligned}$$

Therefore: $1 \equiv 8 \times (-4)$ mod 11, and by taking the residue value, $1 \equiv 8 \times 7$ mod 11

Annex 2. Euler's theorem

We can apply theorem 7.2 to $n = pq$ and conclude that

$$\phi(n) = (p-1)(q-1)$$

counts the number of positive integers $< n$ which are relatively prime to n.

Theorem (Euler's theorem)

Let n be a positive integer and let x be a positive prime to n. Then

$$x^{\phi(n)} \equiv 1 \; (mod \, n)$$

where $\phi(n)$ is the Euler's function.

Proof. Consider the set $\mathbb{Z}_n^* = \{r_1, r_2, \ldots, r_{\phi(n)}\}$, that contains the integers that are relatively prime to n. For any $x \in \mathbb{Z}_n^*$, the modular multiplication by x is a permutation of this set, that is $\mathbb{Z}_n^* = \{xr_1, xr_2, \ldots, xr_{\phi(n)}\}$, because multiplication by x is a function from the finite set $\mathbb{Z}_n^*$ to itself that has an inverse, namely multiplication by $\frac{1}{x}$ (mod n).

Annex 2. Euler's theorem

Proof (cont.) Now, consider the product of all elements of $\mathbb{Z}_n^*$. On one hand, it is $r_1 r_2 \dots r_{\phi(n)}$, on the other hand it is $(xr_1)(xr_2)\dots(xr_{\phi(n)})$. So these products are congruent mod n:

$$\begin{aligned} r_1 r_2 \dots r_{\phi(n)} &\equiv (xr_1)(xr_2)\dots(xr_{\phi(n)}) \pmod{n} \\ r_1 r_2 \dots r_{\phi(n)} &\equiv x^{\phi(n)} r_1 r_2 \dots r_{\phi(n)} \pmod{n} \\ 1 &\equiv x^{\phi(n)} \pmod{n} \end{aligned}$$

where cancellation of the r_i is allowed because all have multiplicative inverses mod n. □

The theorem is a generalization of the little Fermat theorem, that applies for n prime.

Note that Euler's theorem justifies the validity of RSA for any plaintext message x except for $x = p$ or $x = q$ (which anyways are a very small fraction of all possible messges). In those cases, RSA is also valid but the proof requires the use of the Chinese remainder theorem.