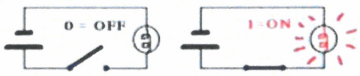
bsv@writeme.com AO@dot.net.by

Massachusetts Institute of Technology (MIT)

Lecture by Pr. Bob Gallagher
Boole (1815-1864) & **Shannon** (1916-2001)



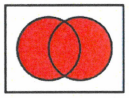
Logical addition (disjunction)

A	B	F=A∨B
0	0	0
0	1	1
1	0	1
1	1	1

A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False

Logical disjunction

OR



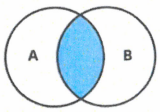
Definition $x + y$

Truth table (0111)

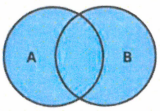
Logic gate

BOOLEAN LOGIC

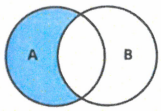
AND Both terms



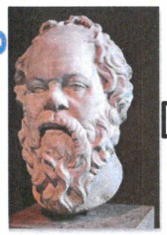
OR Either term



NOT Only one term



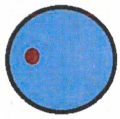
Good logic

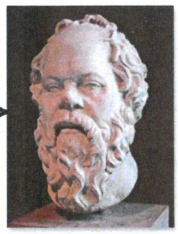


Socrates

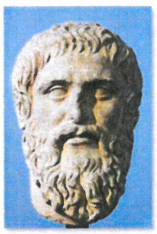
Socrates was a philosopher

$s \in \Phi$

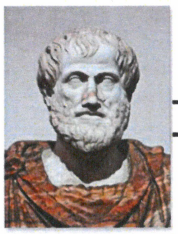




Socrates



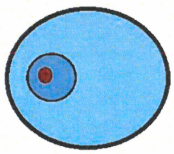
Plato

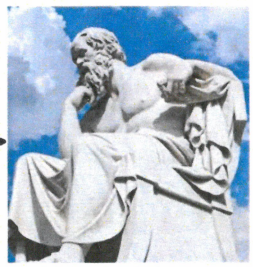


Aristotle

philosophers are men

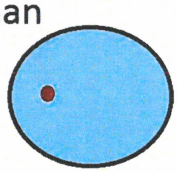
$\Phi \in A$



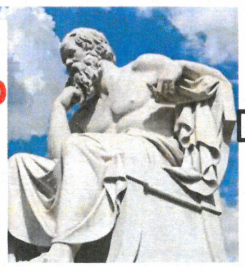


Socrates was a man

$s \in A$

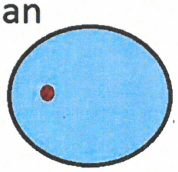


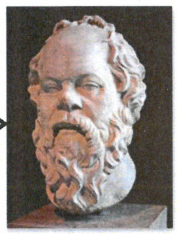
Bad logic



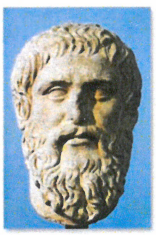
Socrates was a man

$s \in A$

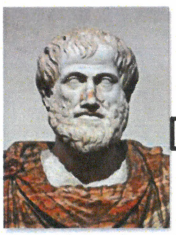




Socrates



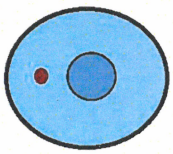
Plato

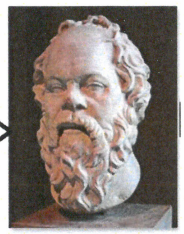


Aristotle

philosophers are men

$\Phi \in A$

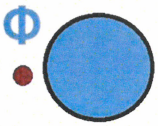


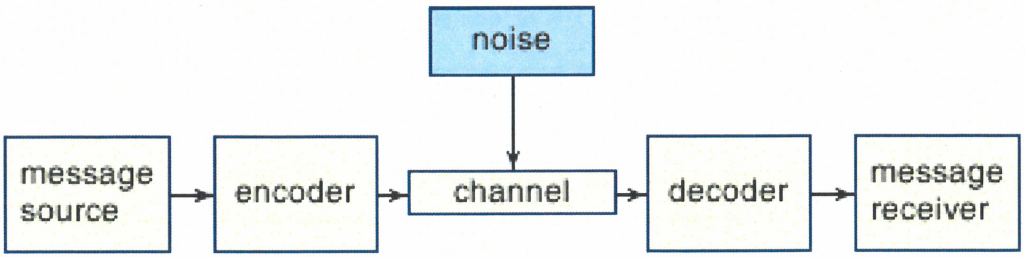


Socrates

Socrates was a philosopher

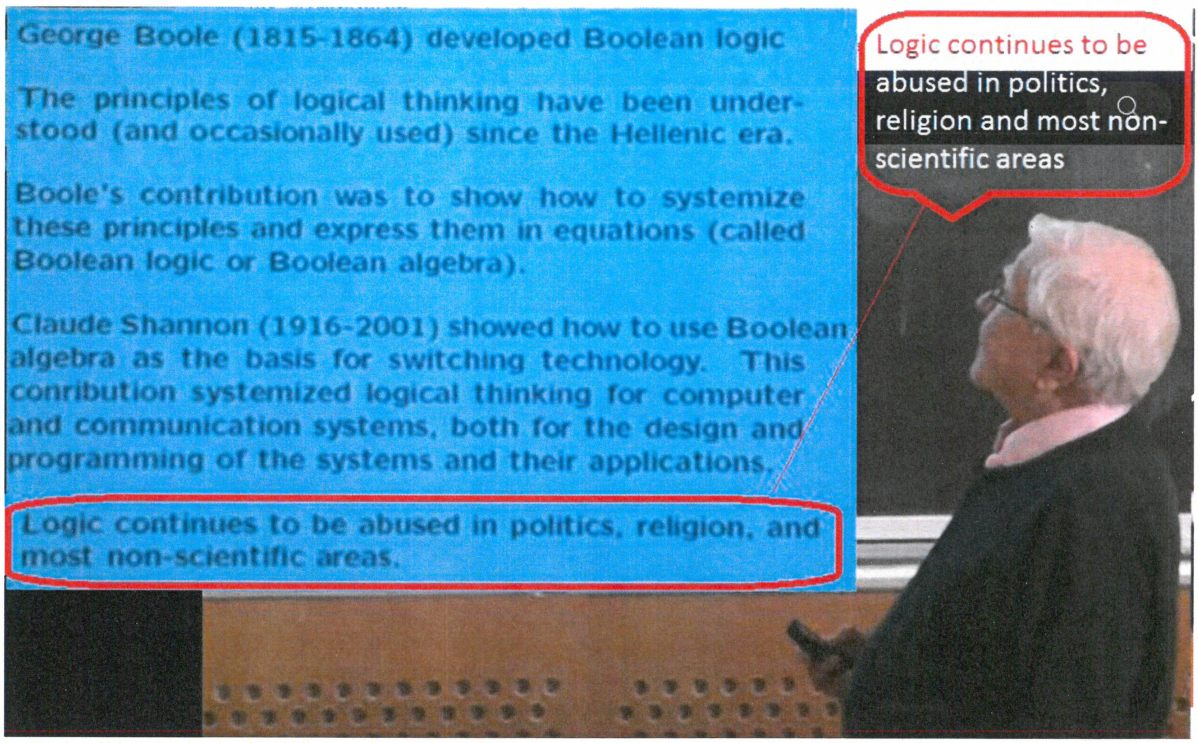
$s \in \Phi$

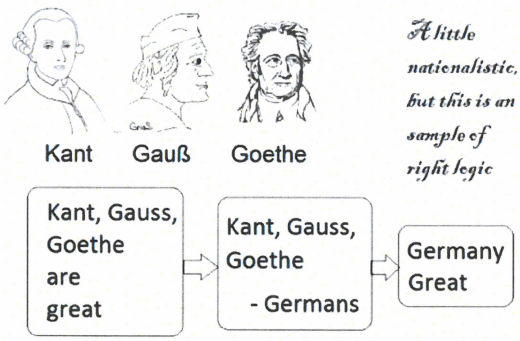


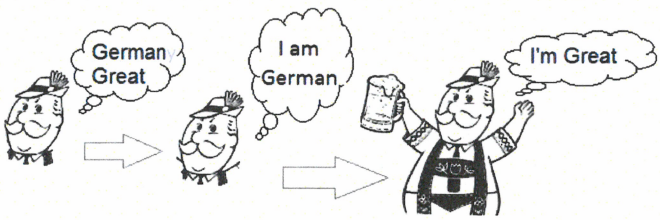


Resume of Lecture by Pr. Bob Gallagher from MIT

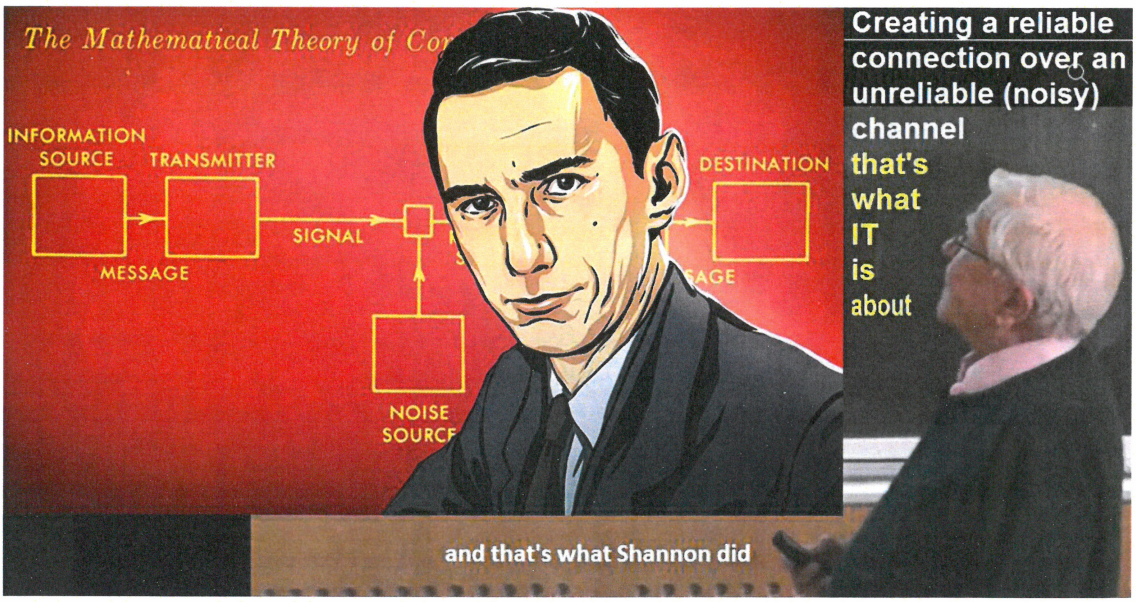
Massachusetts Institute of Technology (MIT)



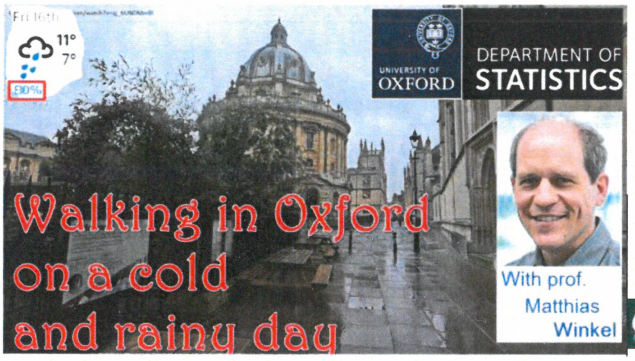




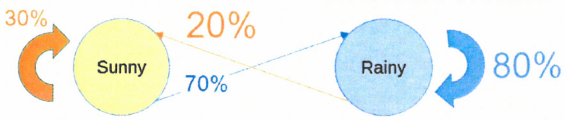
Bad logic (abuse of logic)



	Sun	Rain
Sun	30%	70%
Rain	20%	80%



Markoff Chain Probability Model for Oxford Weather

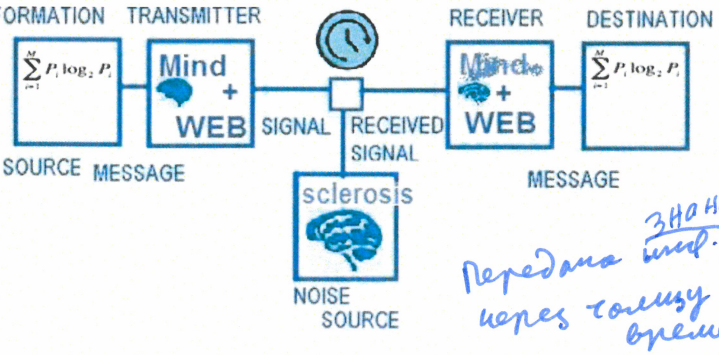


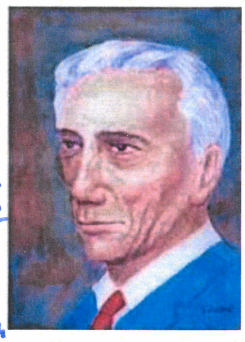
CHALK+TALK ink+think

Good way (1.) listening

(2.) first way of processing

(3.) Writing, incl. sth., you're not quite sure about





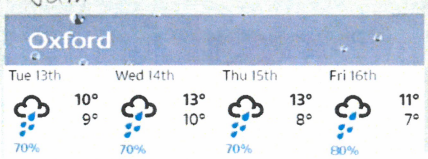
Передача знаний через толщу времени

School ↓gravity↓ MOTION ==formalism==> University $E=MC^2$ $W=2\pi f$ $\int_1^2 \int a\,ds$

Motivation: 80% chance of rain

Let A_j be the event of rain at 9am on day j of this term, $1 \le j \le n$

Suppose the events A_i each have probability p, independently



then take notes on the lecture yourself

80% chance of rain

Let A_j be the event of rain at 9 a.m. on day j this term

$$0 \leq j \leq n$$

Suppose the event A have probability independently P

1. Event and probabilities

Consider an "experiment" which has a set of Ω of outcomes

$$\omega \in \Omega$$

For example

a. tossing a coin $\Omega = \{H \mid T\}$

Head Tail

b. throwing a dice

$$\Omega \{(i,j);\ i,j \in [1,2,3,4,5,6]\}$$

let make them distingwishable  

a red one a blue one

$$\{(i,j);\ i,j \in [1,2,3,4,5,6]\}$$

A subset of Ω is called an event

For example

a) coin comes up tail $A = \{T\}$

b) We observe of total of 9

$A = \{(3,6), (4,6), (5,4), (6,3)\}$ 

If $\omega \in \Omega$ is the outcome, we say that A occur if $\omega \in A$

Compliment of A:

A^c occurs if A does not occur

Union $A \cup B$ occur if A or B occurs (or both)

Intersection: $A \cap B$ occurs if both A and B occurs

Set difference: $A \setminus B = A \cap B^c$ occur if A occurs and B does not occur

A and B are disjoint if

$$A \cap B = \emptyset$$

i.e. A and B cannot occur together

We assign a probability $P(A)$ of each A

Simplest case:

Ω is finite and all outcomes are equally likely

Then $P(A) = \dfrac{|A|}{|\Omega|}$

Probability of any event A

a) $\left.\begin{array}{l} |\Omega| = 2 \\ |A| = 1 \end{array}\right\} \Rightarrow P(A) = \dfrac{1}{2}$ H T

b) $\left.\begin{array}{l} |\Omega| = 36 \\ |A| = 4 \end{array}\right\} \Rightarrow P(A) = \dfrac{4}{36} = \dfrac{1}{9}$

Elementary combinatorics

Arrangements of distinguishable or different objects

Suppose we have n distinguishable objects

? How many ways are there to order them? (permutation)

e.g. $1, 2, 3, 4, \dots n$

or $n, n-1, n-2, \dots 2, 1$

There are n options for ordering the first objects

then $n-1$ — 2nd —

inductively $n-(m-1)$ — m^{th}

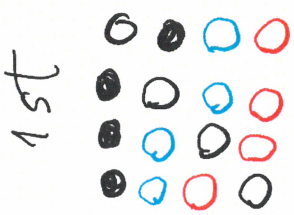
until n^{th}

So in all there are

$n(n-1)\dots 2\cdot 1 = n!$ Permutations

Example

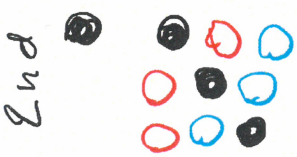
m 1st 2nd 3rd 4th



There are n options for the 1st object

or n positions

Once you've chosen the 1st object



$n-1$ remaining options for 2nd object

GALOIS

arrangent of 3 vovels and then 3 consonants

If Ω is the set of all arrangements and $A \subseteq \Omega$ the set of arrangements with all vovels before all consonants, then

$$P(A) = \frac{|A|}{|\Omega|} = \frac{3! \cdot 3!}{6!} = \frac{36}{720} = \frac{1}{20}$$

So you can try the same with other words

3rd

$\underbrace{\quad}_{2}$ $n-2=2$ $n-2$ options for the 2nd

4th

So $n-$ 1st

$n-1$ - 2nd

$n-(m-1)$ 3rd

until 1 — last n^{th} 4th

Example

There are 6! ways to order the letters of GALOIS

Evariste Galois
(20: 1811 – 1832)
French math

If randomly reorder the letters what is probability that the vowels (A, O, I) are all before consonants? (G, L, S)

"uniformly of random"

There are $3! * 3! = 36$

Arrangements when not all objects are indistinguishable

How many different arrangemens of A, A, A, B, C, D

If we had

$A_1\ A_2\ A_3\ B\ C\ D$ there would be 6! orderings

$B\ A_2\ D\ A_1\ A_3\ C$

$B\ A\ D\ A\ A\ C$

$B\ A_1\ D\ A_2\ A_3\ C$

correspond to the same ordering of A A A B C D

Each one is one of 3! which differ only in the order of $A_1\ A_2\ A_3$

So the 6! fall into groups of size 3! which are indistinguishable if $A_1 = A_2 = A_3 = A_4$

We want to count the number of groups which is $\frac{6!}{3!}$

Generalizations

The number of the N objects

$$\underbrace{x_1, \ldots, x_1}_{m_1}, \underbrace{x_2, \ldots, x_2}_{m_2}, \ldots, \underbrace{x_k, \ldots, x_k}_{m_k}$$

where $n = m_1 + m_2 + \ldots + m_k$

$$\frac{n!}{m_1!\, m_2! \cdots m_k!}$$

Case $k = 2$

\# Ordering of $\underbrace{v, v, \ldots, v}_{m}\ \underbrace{x, x \ldots x}_{n-m}$

is $$\frac{n!}{m!\,(n-m)!} = \binom{n}{m} = \binom{n}{n-m}$$

binomial coefficient

Binomial coefficient (which you have written as ${}^{n}C_{m}$)

But here in Oxford we very much like this way of writing $\boxed{\binom{n}{m}}$

That binomial coefficient is something that you are familar with and it usefull in many way, not just in order to find arrangements of objects, but also to choose M of the given objects from the total N.

And you can do that with tics V and crosses X

for example to work out how many are there to form football team of size M from squad of size N just by identifying football team as the players where you assign a tick V whereas the other players are assign as X and so counting

John X
Jack V
Mike V
⋮
Tom X
Frank V

Football Team.

how many ways there are to select team is exactly the same as number of ways to order the order the tics $\boxed{\checkmark}$ and crosses $\times$ but I haven't got time to write that

I leave you with that to maybe think about more, if you haven't put this together at this stage

So this leave us to say:
what about

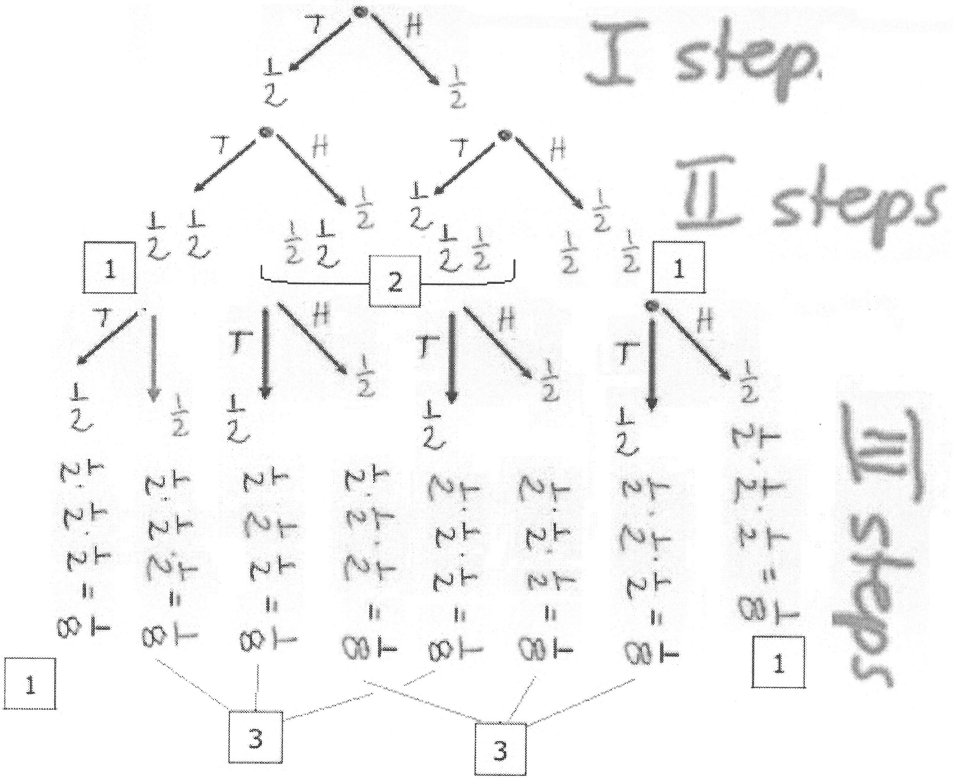
"80% chance of rain on Friday"

I will see you later on next lection... anyway

Oxford

1								1
1	1							2
1	2	1						4
1	3	3	1					8
1	4	6	4	1				16
1	5	10	10	5	1			32
1	6	15	20	15	6	1		64
1	7	21	35	35	21	7	1	128

Pascal's triangle



$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2+2ab+b^2$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$

$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$$

$$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

Proto-language

Tower of Babel

Old Slavic

Ancient Greek ?
Ελληνικά

Ancient Hebrew
עברית

RU
EN
FR
DE
learn

Esperanto
international auxiliary language

Mia nomo estas Andy.
Du plus du estas kvar

Cross-platform Java

bytecode

Hello.java => javac.exe = Hello.class

JVM → Intel CPU

JVM → AMD CPU

JVM → Apple CPU

bytecode

```
Method Add()
  0 aload_0
  1 invokespecial
                #1
  <Method
java.lang.Object()>
  4 return
```

Sun microsystems
Java

trial
0.7 billion

Microsoft

~~J++~~ → C#

JIT-compiler

exe

Hello.cs => csc.exe = Hello.~~class~~

C# компилятор

IL
Intermediate Language

JVM → Intel CPU

JVM → AMD CPU

JVM → Apple CPU

Hello.vb => vbc.exe = Hello.~~class~~ .exe

VB компилятор

CIL - Common Intermediate Language

```
void .ctor() {
  .maxstack  1
  IL_0000:  ldarg.0
  IL_0001:  call instance
void
   System.Object::.ctor()
  IL_0006:  ret
} // end of
     method Add::.ctor
```

Hello.pl=> plc.exe = Hello.~~class~~ .exe

After him I love

More than I love these eyes,
more than my life,
More, by all mores,
than e'er I shall love wife

Windows Kernel

JMP -CorEXEMain

CIL (named .EXE)

```
class Dog
{
  public string name;
  public string bread;
  public int age;
```


```
  public void Bark()
  {
    Console.WriteLine("Woof woof!");
  }

static void Main(string[] args)
{
    Dog dori = new Dog();  //Constructor works
    dori.age = 3;

    dori.name = "Dori";
    dori.breed = "Mongrel";
    dori.Bark();
}
```

```
public Dog()
{
}
public Dog(string name)
{
    this.name = name;
}
public Dog(string name, string breed)
{
    this.name = name;
    this.breed = ref breed;
}
```

1 - **constructor** no returns value

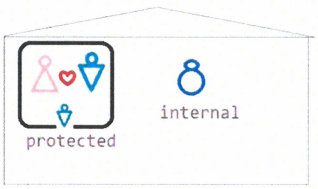
2. The name of the **constructor** is the same name is the class.

3. more than one **constructor**

private protected internal


```
class AFather
{
   protected string name;
   int age;
}
class ASon:AFather
{
    public ASon(string name)
    {
       base.age = 33;
       base.name = name;
    }
}
```

unavailable available




```
class Program
{
    static void Main(string[] args)
    {
        AFather af = new AFather();
        ASon andy = new ASon("Olaf");
    }
}
```

Program.exe

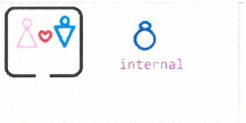
```
class AFather
{
   protected string name;
   internal int age;
}

class Program
{
    static void Main(string[] args)
    {
        AFather af = new AFather();
        af.age = 33;
        ASon andy = new ASon("Olaf");
    }
}
```

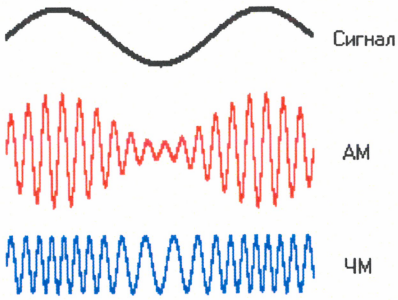
available
unavailable

ASon.dll

```
class ASon:AFather
{
    public ASon(string name)
    {
       base.name = name;
       base.age = 33;
    }
}
```

Reginald A. Fessenden
(October 6, 1866 – July 22, 1932)

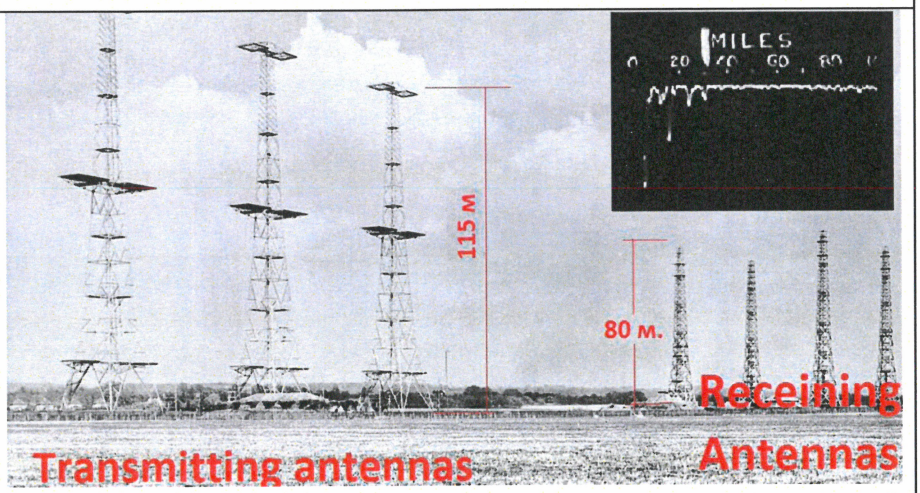


(October 6, 1866 – July 22, 1932)

first transmission of speech by radio (1900), and the first two-way radiotelegraphic communication across the Atlantic Ocean (1906)

"Ни одна организация, занимающаяся какой-либо конкретной областью деятельности, никогда не изобретает какие-либо важные разработки в этой области или не внедряет какие-либо важные разработки в этой области до тех пор, пока она не будет вынуждена сделать это из-за внешней конкуренции.." Oxford University Press. The Quarterly Journal of Economics , Feb., 1926, p. 262.

Battle of Britain
(3 month 3 weeks)
10.07-31.10.1940



Radar played a major role in the Battle of England

H. Nyquist

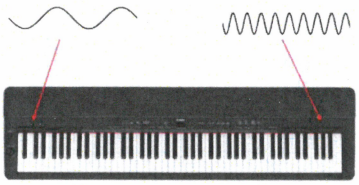
$$W = K \log m$$

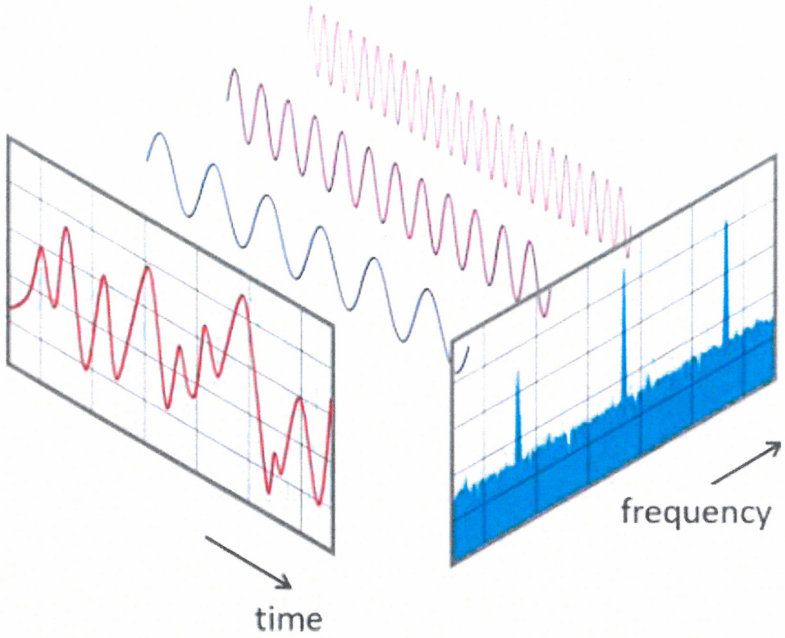
Where W is the speed of transmission of intelligence,
m is the number of current values,
and, K is a constant.

Ralph **Hartley**
(81:1888-1970)

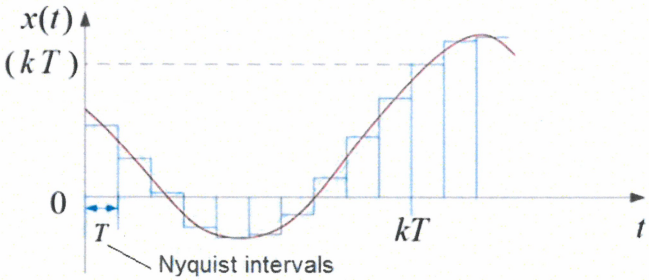
$$H = n \log s$$
$$= \log s^n.$$

Fourier transform

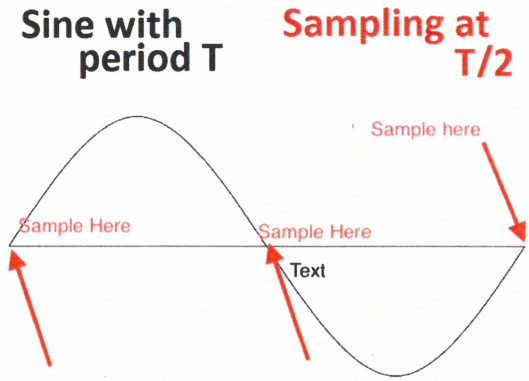


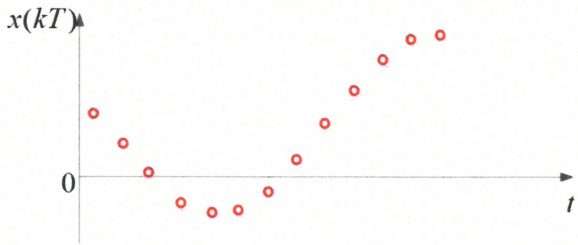


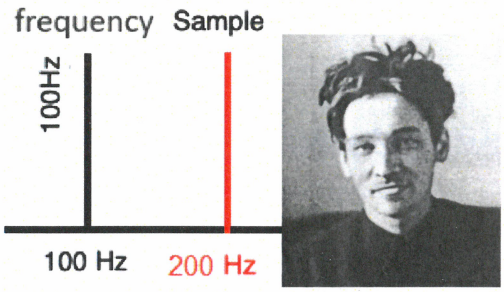
Sampling. Kotelnikov-Nyquist Theorem

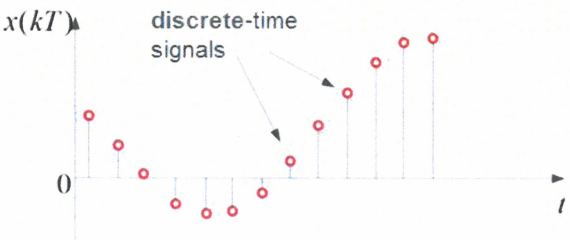


Time intervals T, through which readings s (kT) are taken, are called Nyquist intervals.





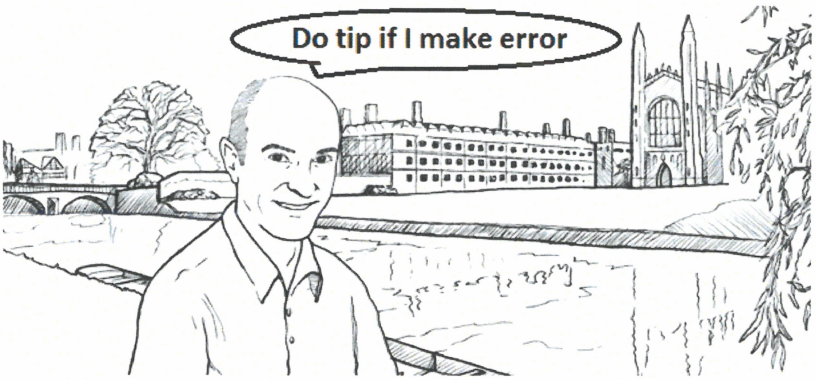




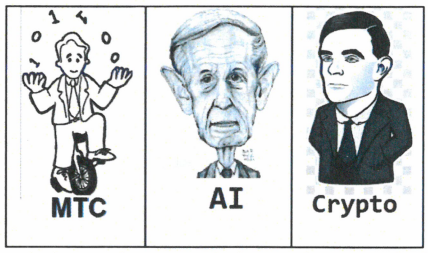
$$F_{sample} >= 2 * F_{max}$$

$$(T_{sample} <= T_{min}/2)$$

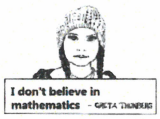
Котельников

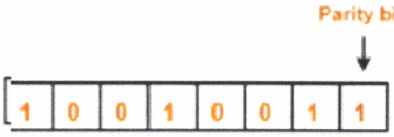


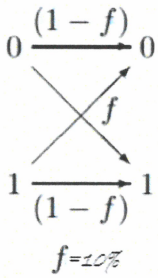
Sir **Dr. D. MacKay**,
University of Cambridge
(22 April 1967 – 14 April 2016)

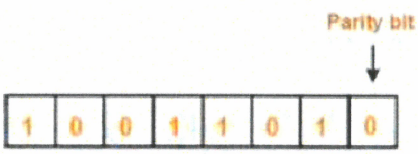


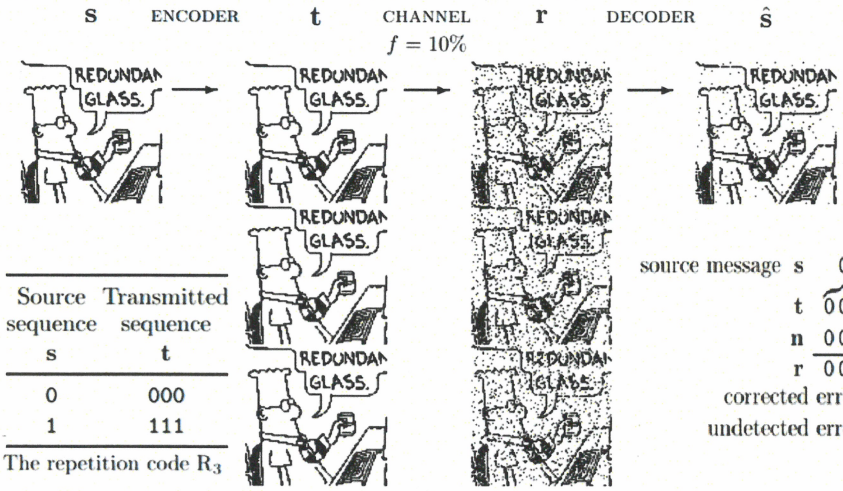
"I believe in clean energy,
but I also believe in mathematics"











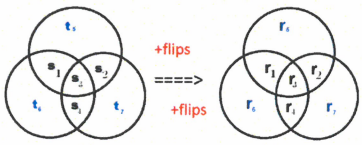
Source sequence s	Transmitted sequence t
0	000
1	111

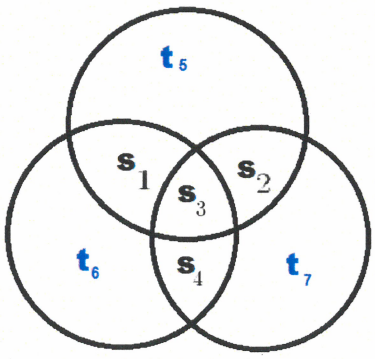
The repetition code R_3

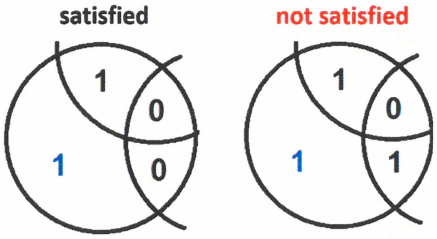
source message s	0	0	1	0	1	1	0
t	000	000	111	000	111	111	000
n	000	001	000	000	101	000	000
r	000	001	111	000	010	111	000
corrected errors		*					
undetected errors					*		

7.4. Hamming code.

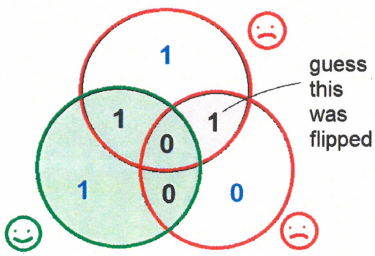
$$\frac{4}{\Sigma} \rightarrow \frac{7}{t}$$

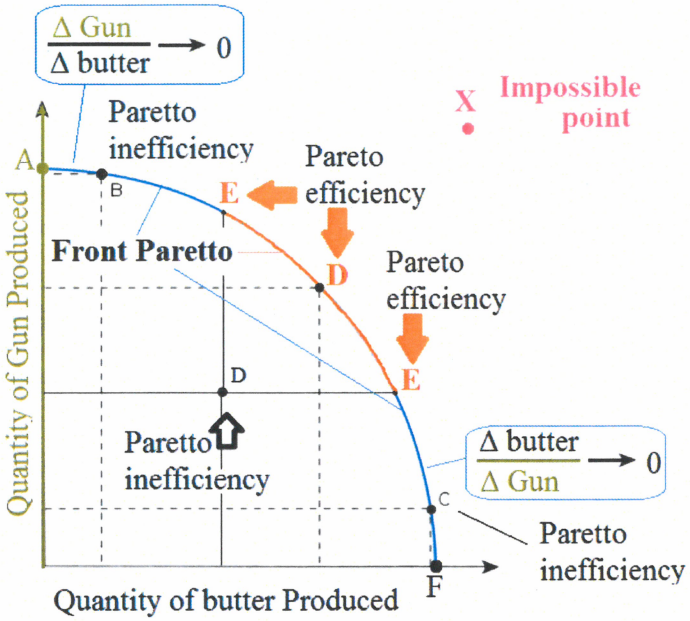






1+1+0+0=**0** 1+1+0+1=**1**

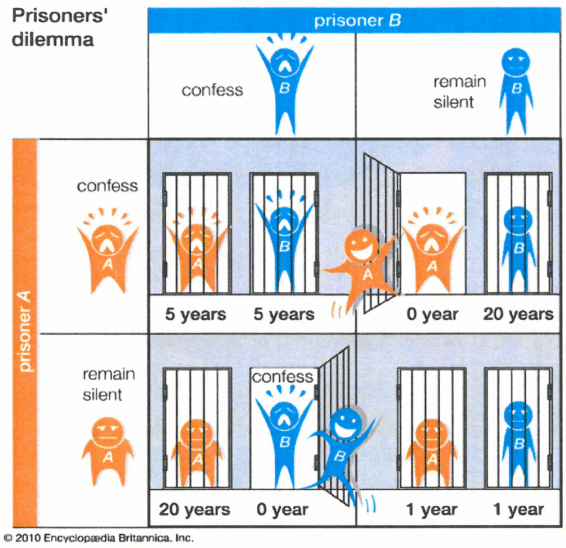


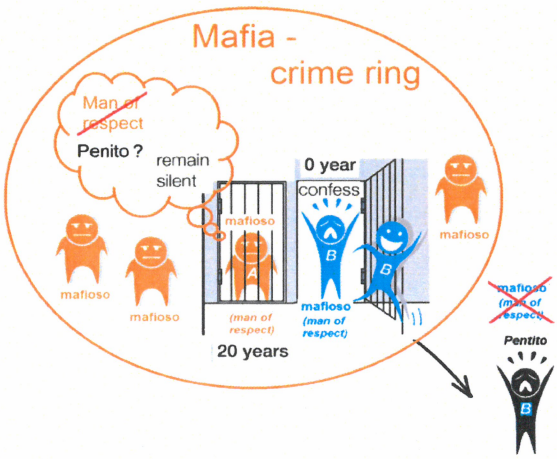


by Vilfredo Pareto

1848-1923

The orange sector E-D-E is the most Pareto efficient - since an increase in one indicator leads to a decrease in another.





Game Theory

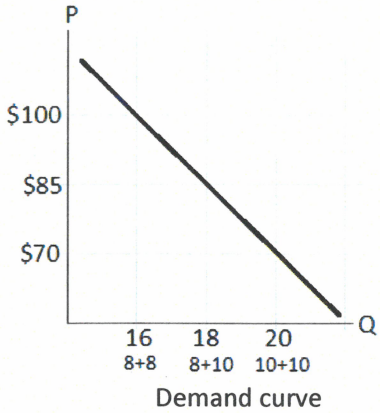
Nash Equilibrium

** => Nash equilibrium

$H_2(x)$ / $H_1(x)$	Player 2	Recognition;	Non-recognition;
Player 1		1	2
Recognition;	1	* -5 / -5 *	-20 / 0
Non-recognition;	2	0 / -20	-1 / -1

-1-1

Pareto Optimality

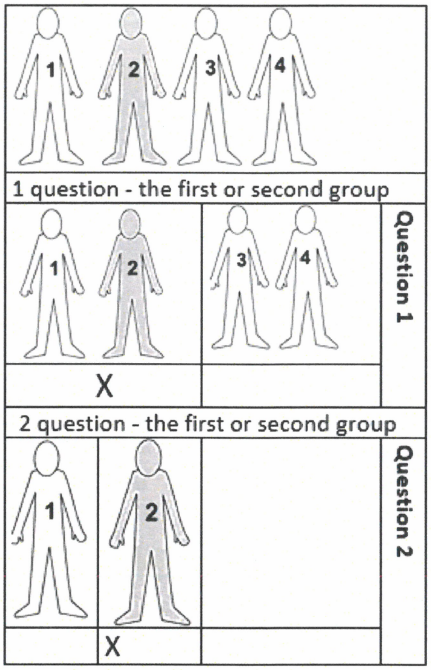


	Barrel	1.	2.
		$8 \cdot 10^6$ / day	$10 \cdot 10^6$ / day
1.	$8 \cdot 10^6$	$800 millions per day $100 $800 millions per day	$850 millions per day $85 $680
2.	$10 \cdot 10^6$ / day	$680 millions per day $85 $850 millions per day	$700 millions per day $70 $700 millions per day

Say **NO** to the **first**

Say **YES** to the **second** if it is better than the first

Say **NO** to the **third** only if it is worse than all the others



Average number of questions =

2*0.25+ **2***0.25+ **2***0,25+ **2***0,25 =**2**

Average number of questions =

1*0.5+	2*0.25+	3*0,125+	3*0,125
			

Question 1. Is this Zuckerberg?	 50%	1*0.5
Question 2. Is this Sergey Brin?	 25%	2*0.25
Question 3. Is this Stefan from BMW?	 12,5%	3*0,125
So Prince Saud	 12,5%	3*0,125
Average number of questions = **1,75**		

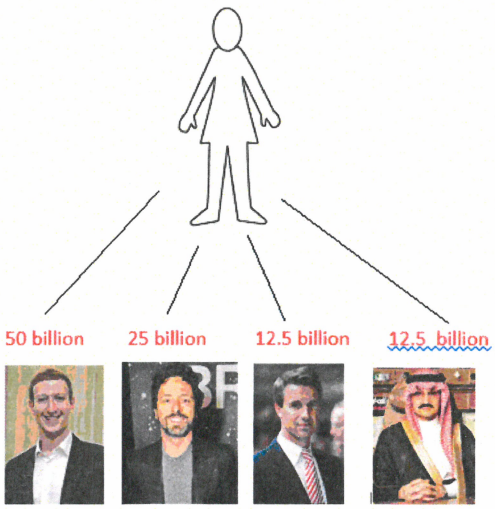
Quantifying information

$$S(x) = \sum_{i=1}^{n} p(i) \log_2 \frac{1}{p(i)}$$

Quantifying information

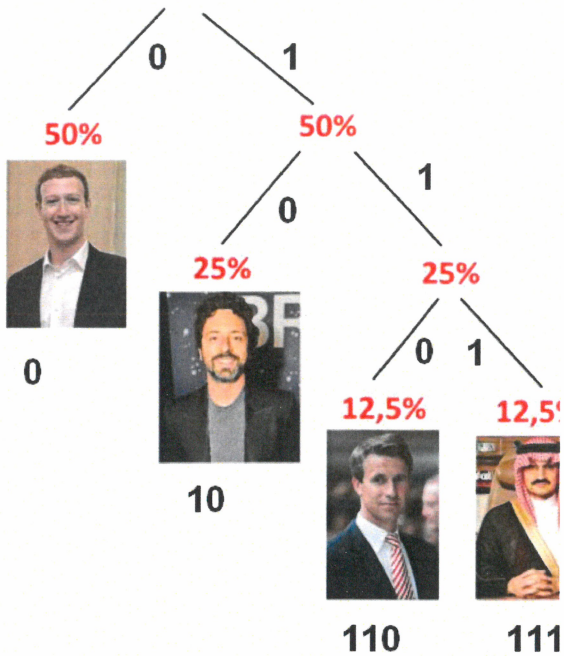
$$I(x_i) = \log_2\left(\frac{1}{p_i}\right)$$

number of bits required to encode choice



ce

Huffman code

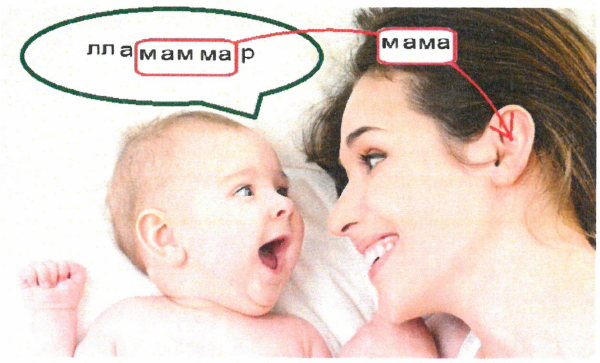


First-order approximation (symbols independent but with frequencies of Belarusian txt).

Мама мыла ра

М - 3	30%	1-3	М
а - 4	40%	4-7	а
ы -1	10%	8	-ы
л - 1	10%	9	-л
р - 1	10%	10	-р
10			

лла мамма р



Second-order approximation (digram (2-symbols) structure as in Belarusian)

Мама мыла ра

Ма - 2	22%	1-2	ма
ам - 2	22%	3-4	ам
мы - 1	11%	5	мы
ыл - 1	11%	6	ыл
ла - 1	11%	7	ла
а р - 1	11%	8	ар
ра - 1	11%	9	ра
9			

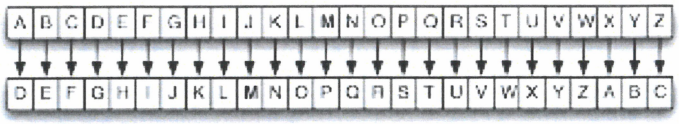
0. 4 6 7 3 1 9 1 6 7 3 5

ам ыл ла ам ма ра ма ыл ла ам мы

мылла рама

Caesar Cipher

C=(p+3) mod 26



- We can use the ordinal positions of letters in a cipher to generate this key:

A	B	C	D	...	Y	Z
1	2	3	4	...	25	26

- We can also rotate the starting point. If we add 3 to every number, we might use this key:

A	B	C	D	...	Y	Z
4	5	6	7	...	2	3

ABBA

↓

DEED

Vigenere Cipher

An improvement we can make to the Caesar cipher is to increase the number of keys.

While the Caesar cipher uses a single key, the **Vigenere** cipher uses multiple keys by selecting a keyword.

In the Vigenere cipher, for each new letter of message, it is enciphered using a different letter of the keyword.

https://www.youtube.com/watch?v=BgFJD7oCmDE

To encrypt the message **ABBA** using the keyword **LAW**, we might come up with the following table:

Plaintext	A	B	B	A
Ordinal Position	1	2	2	1
Keyword (LAW)	L	A	W	L
Keyword Ordinal Position	12	1	23	12
Sum	13	3	25	13
Ciphertext	M	C	Y	M

Frequency Analysis https://www.youtube.com/watch?v=sMOZf4GN3oc Khan

- Another issue with Caesar ciphers is that an adversary may be able to crack the code without a pin.
- For example, if we see a single letter word in the message, we might be able to guess that the character or number represents I or A. From there, we might be able to discover some patterns in the message.
- A pattern may be how frequently letters appear in the English language.

A	B	C	D	E	F	G	H	I	J	K	L	M
8.1%	1.5%	2.8%	4.3%	12.7%	2.2%	2.0%	6.1%	7.0%	0.2%	0.8%	4.0%	2.4%

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.7%	7.5%	1.9%	0.1%	6.0%	6.3%	9.1%	2.8%	1.0%	2.4%	0.2%	2.0%	0.1%

- Some letters appear very frequently, such as E or T and some letters appear very infrequently, such as J or K. Using these frequencies, we can look at what appears frequently or infrequently in the cipher-text and perhaps find certain patterns.
- While for humans it might be tedious to conduct frequency analysis to decode a message, a computer can do it very quickly.