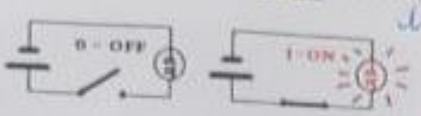
Massachusetts Institute of Technology (MIT)

Lecture by Pr. Bob Gallagher

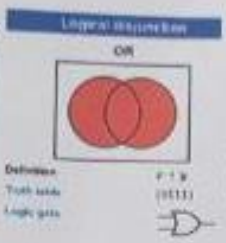
Boole (1815-1864) & **Shannon** (1916-2001)



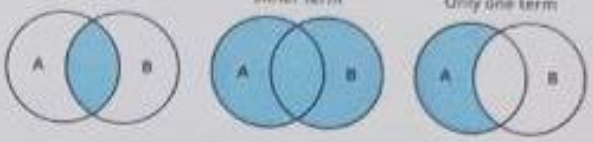
Logical addition (disjunction)

A	B	F=A∨B
0	0	0
0	1	1
1	0	1
1	1	1

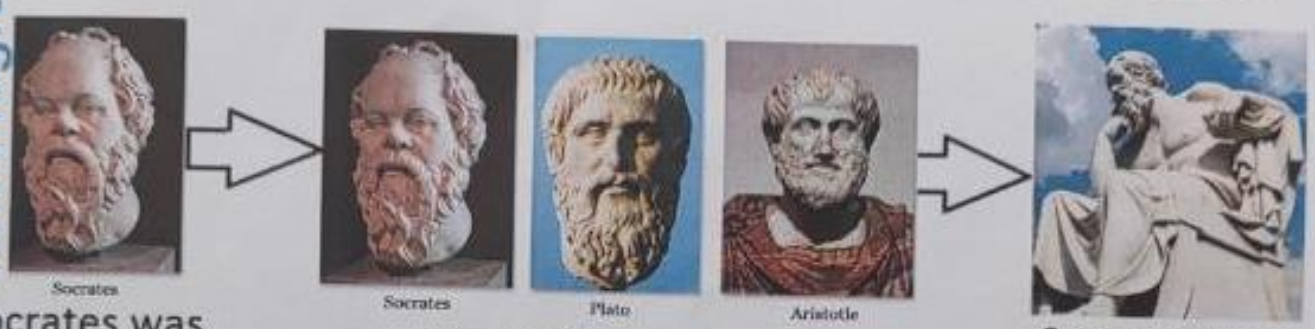
A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False



BOOLEAN LOGIC



Good logic



Socrates was a philosopher

philosophers are men

Socrates was a man

Bad logic

Socrates was a man

philosophers are men

Socrates was a philosopher

Resume of Lecture by Pr. Bob Gallagher from MIT

Massachusetts Institute of Technology (MIT)

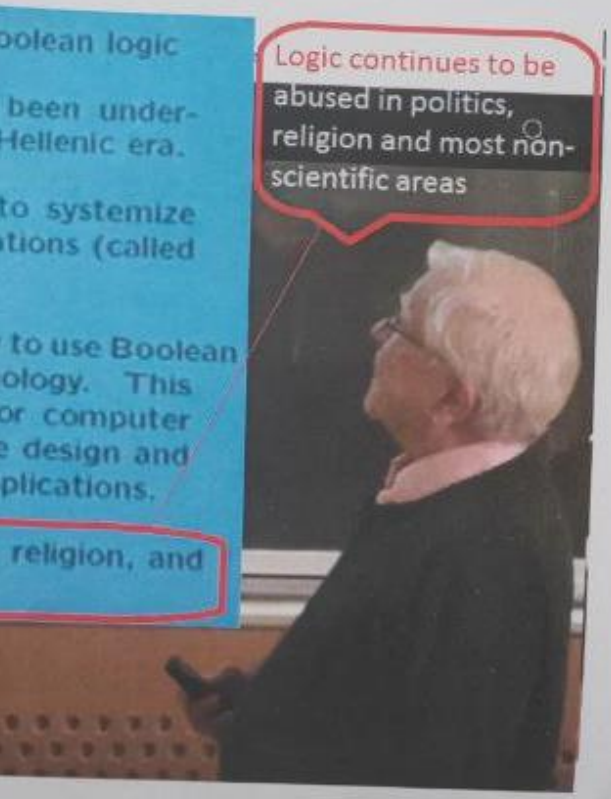
George Boole (1815-1864) developed Boolean logic

The principles of logical thinking have been understood (and occasionally used) since the Hellenic era.

Boole's contribution was to show how to systemize these principles and express them in equations (called Boolean logic or Boolean algebra).

Claude Shannon (1916-2001) showed how to use Boolean algebra as the basis for switching technology. This conribution systemized logical thinking for computer and communication systems, both for the design and programming of the systems and their applications.

Logic continues to be abused in politics, religion, and most non-scientific areas.

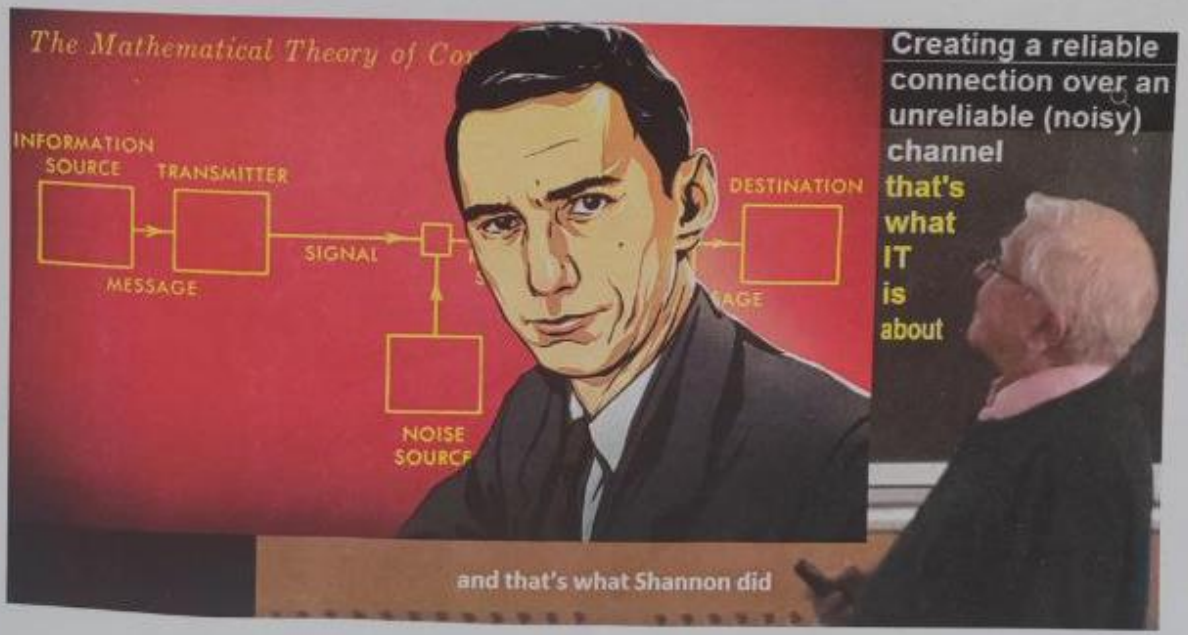


A little nationalistic, but this is an example of right logic

Kant, Gauss, Goethe are great → Kant, Gauss, Goethe - Germans → Germany Great

Bad logic (abuse of logic)

национализм



Як вывучыць новую мову – замежную ці мову праграмавання. Гэта залежыць ад шматлікіх фактараў: перш за ўсё, ад наяўнасці часу, які вы гатовыя выдаткаваць на вывучэнне мовы праграмавання C# і платформы .NET Framework (або Core). Нарэшце, здольнасці мець важна, але, на маю думку, гэта не галоўнае.

19 лютага 2024 г. – 23 лютага 2024 г.
https://bsu.by/news/nedelya-rodnogo-yazyk_a-start/uet-v-bgu-d/

Kató Lomb (94: 8.2.1909 9.6.2003

Ёсць аналогія з вывучэннем замежнай мовы. Адна з першых у свеце сінхронных перакладчыкаў Като Ломб - яна раіла перад вывучэннем замежнай мовы даведацца, ці можна выдзяляць на заняткі хаця б 10-12 гадзін у тыдзень на працягу 2-х гадоў (ўсяго 1040-1248 гадзін). Калі не - і не падманвайце сябе.
Яе 10 запаведзяў па арганізацыі вывучэння натуральных моў з кнігі «Як я вывучаю мовы» (прыведзены ў дадатку), на мой погляд, актуальныя і для вывучэння моў шляхам праграмавання.

Адказаць на гэтае пытанне Вам дапаможа гэты тэсцік.
Выконваць яго трэба самастойна, на працягу 3-5 дзён.
Ад таго, колькі пунктаў Вы пройдзеце залежыць ад выбару хуткасці, з якой можна працаваць. Запускаць усе каманды лепш з кансолі Start|Run|cmd.
ПРАДМОВА. Адзін са стваральнікаў праекту Apple Macintosh. Джэф Раскін (61:09.03.1943 - 26.02.2005) высунуў на мой погляд зусім правільны лозунг **Your Time Is Sacred; Your Work Is Sacred** - з гэтага вынікае, што ў абавязковым парадку неабходна захоўваць праведзеную працу - яна святая, і час, на яе выдаткаваны, бясцэнны. ***[Jef Raskin. THE HUMAN INTERFACE. Chapter 1.6]***.

«Прыблізна кожную гадзіну я ствараю рэзервовую копію сваёй працы з дапамогай энерганезалежнай запамінальнай прылады, якая можа быць фізічна вынята з кампутара і такім чынам абаронена ад любых нечаканасцяў у яго працы.
Акрамя таго, кожны тыдзень я захоўваю рэзервовую копію сваёй сістэмы на вонкавым дыску.
Гэта не значыць, што я параноік, - я ўсяго толькі лічу, што такі падыход практычны…
Сістэма павінна разглядаць дадзеныя, якія ўводзяцца юзэрам, як неацэнныя»

JEF RASKIN

10 запаведзяў К.Ломб - чалавека, які ведаў 16 моў

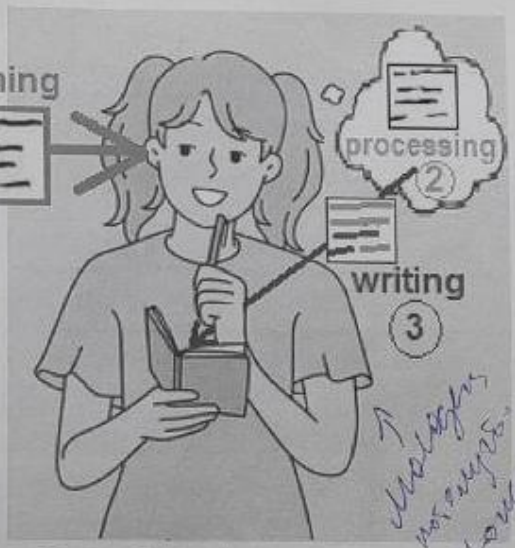
1. Займайся мовай штодня. Калі ўжо зусім няма часу, дык хаця б дзесяць хвілін. Асабліва добра займацца раніцай.
2. Калі жаданне займацца занадта хутка слабее, не «фарсіруй», але і не кідай вучобу. Прыдумай якую-небудзь іншую форму: адкладзі кнігу і паслухай радыё, пакінь практыкаванні падручніка і пагартай слоўнік і г.д.
3. Ніколі не зубры, не завучвай нічога па асобнасці, у адрыве ад кантэксту.
4. Выпісвай па-за чаргой і завучвай усе "гатовыя фразы", якія можна выкарыстоўваць у максімальна магчымай колькасці выпадкаў.
5. Старайся разумова перакладаць усё, што магчыма: прамільгнулае рэкламнае табло, надпіс на афішы, абрыўкі выпадкова пачутых размоў. Гэта заўсёды адпачынак, нават для стомленай галавы.
6. Вывучваць трывала варта толькі тое, што выпраўлена выкладчыкам. Не перачытвай уласных нявыпраўленых практыкаванняў: пры шматразовым чытанні тэкст запамінаецца мімаволі са ўсімі магчымымі памылкамі. Калі займаешся адзін, то вывучвай толькі загадзя правільнае.
7. Гатовыя фразы, ідыяматычныя выразы выпісвай і запамінай у першай асобе, адзінага ліку. Напрыклад: "I am only pulling your leg" (Я цябе толькі дражню).
8. Замежная мова - крэпасць, якую неабходна штурмаваць з усіх бакоў адначасова: чытаннем газет, слуханнем радыё, праглядам недубляваных фільмаў, наведваннем лекцый на замежнай мове, прапрацоўкай падручніка, перапіскай, сустрэчамі і гутаркамі з сябрамі - носьбітамі мовы.
9. Не бойся казаць, не бойся магчымых памылак, а прасі, каб іх выпраўлялі. І галоўнае, не хвалюйся і не крыўдуй, калі цябе сапраўды пачнуць папраўляць.
10. Будзь цвёрда ўпэўнены ў тым, што ў што б там ні стала дасягнеш мэты, што ў цябе нязломная воля і незвычайныя здольнасці да моў.

Markoff Chain Probability Model for Oxford Weather

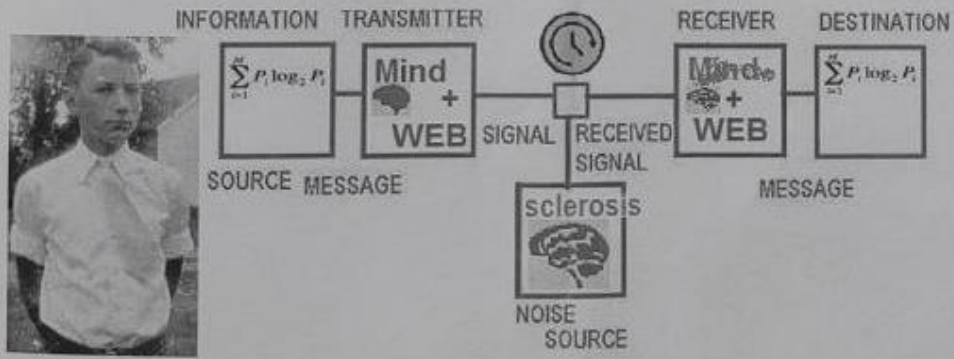
CHALK + TALK

ink + think

Bad way



Good way
1. listening
2. first way of processing
3. **Writing,** incl. sth., you're not quite sure about



School Motion ==formalism==> University

Motivation: 80% chance of rain

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

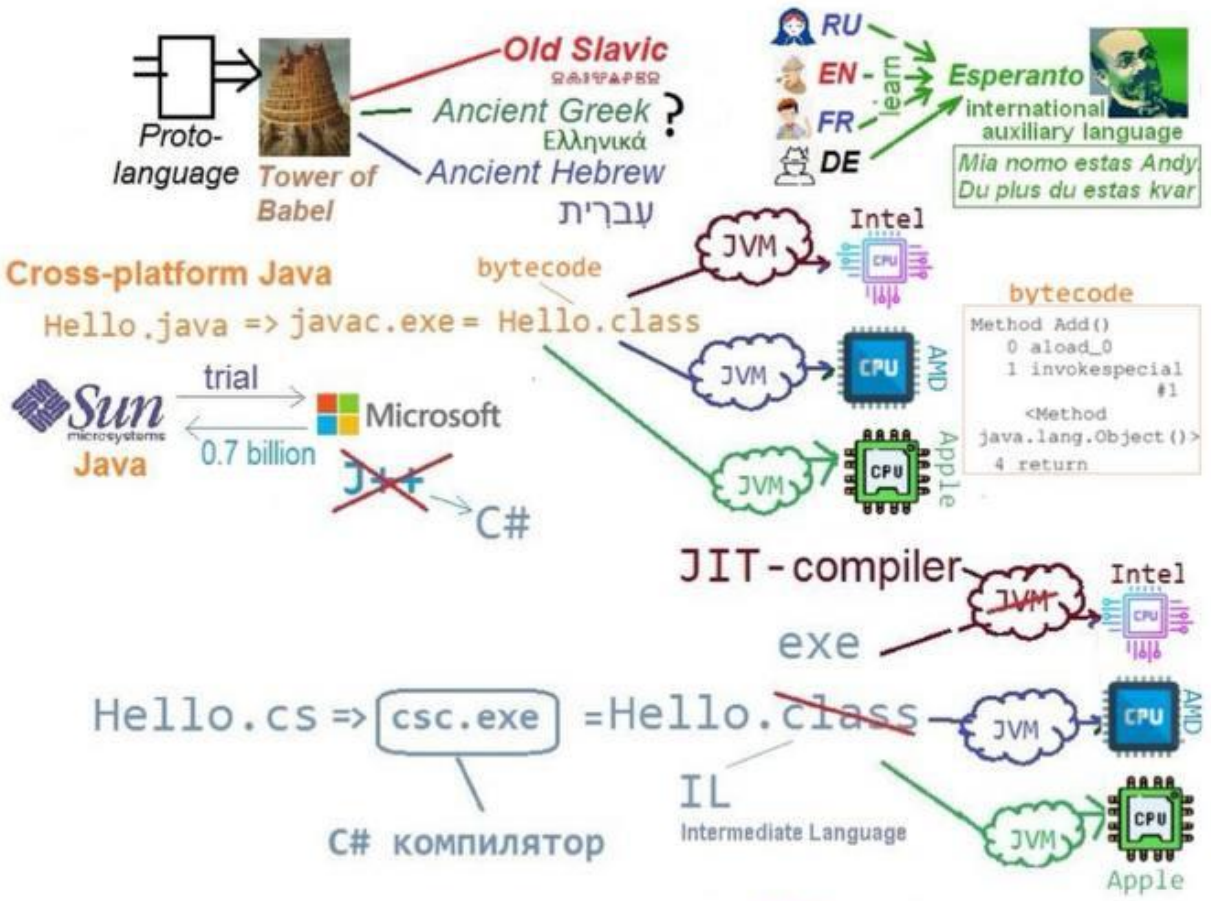
Suppose the events A_j each have probability p, independently

then take notes on the lecture yourself

GALOIS

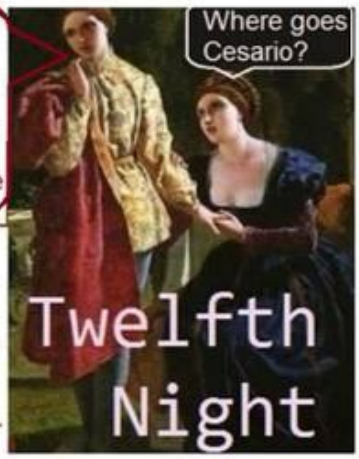
$G = ?\cdot S$

$(n \cdot m / m$



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

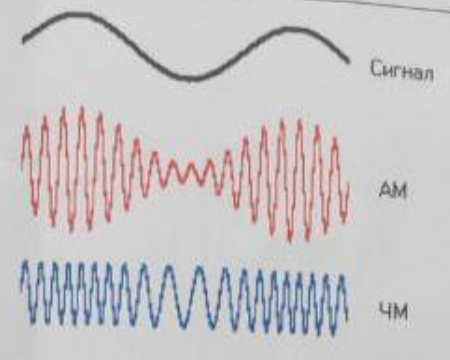


Windows Kernel

JMP -CorEXEMain

CIL (named .EXE)

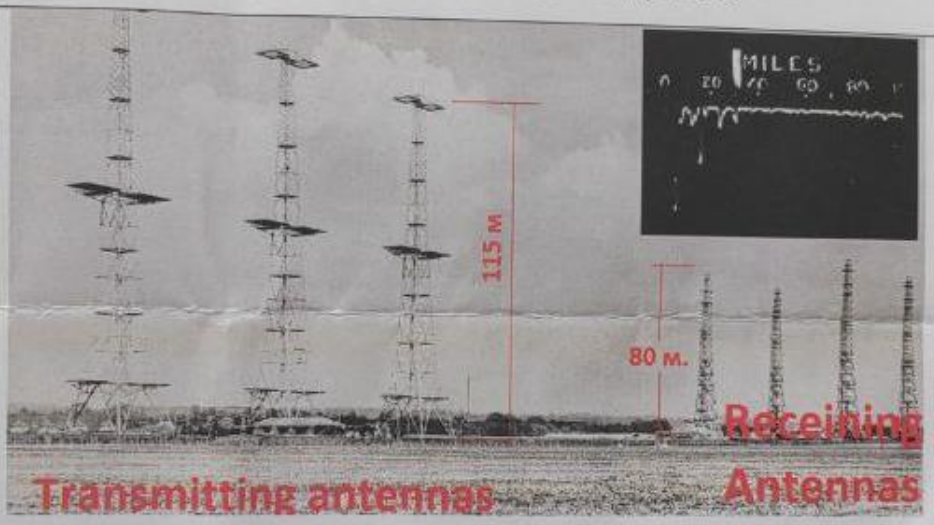
Reginald A. Fessenden
(October 6, 1866 – July 22, 1932)



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)

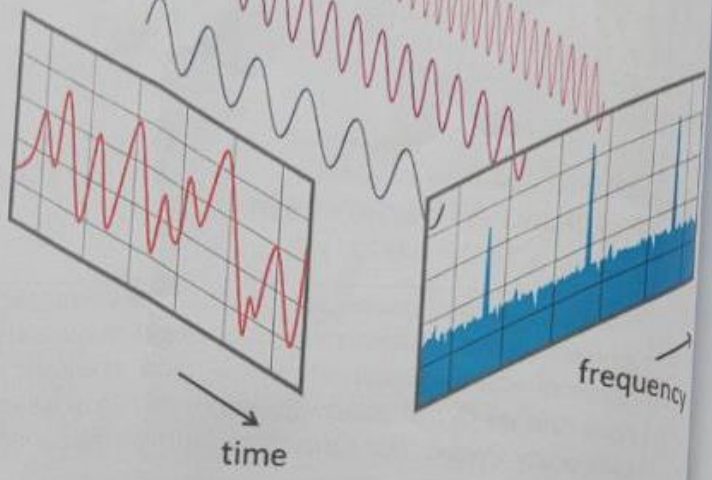
$$H = n \log s = \log s^n.$$

$e^{-j\pi} = -1$

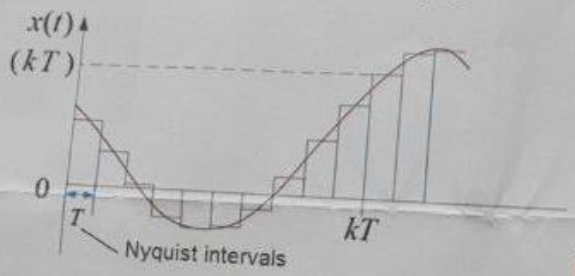
Любой сигнал можно разложить на простейшие гармоники

Fourier transform

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-i2\pi\xi x}\, dx.$$



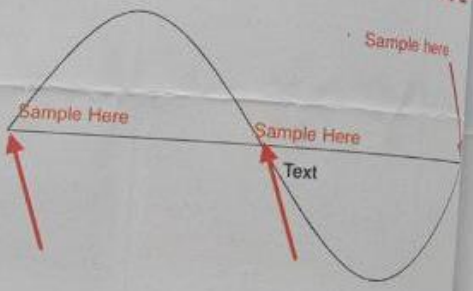
Sampling. Kotelnikov-Nyquist Theorem

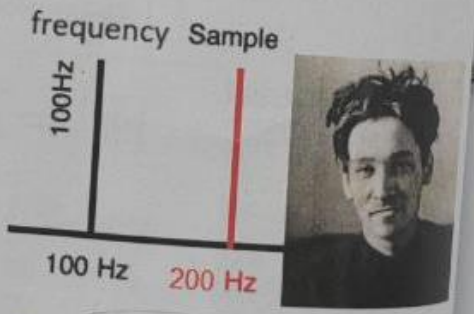


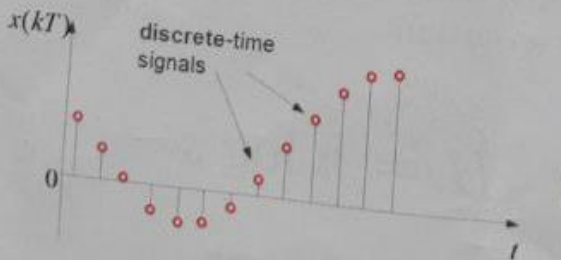
Time intervals T, through which readings s (kT) are taken, are called Nyquist intervals.

Sine with period T

Sampling at T/2







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

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

$$x(t) = \sum_{k=-\infty}^{\infty} x(k\Delta t)\, \frac{\sin 2\pi F(t-k\Delta t)}{2\pi F(t-k\Delta t)}$$

$y(t) = 2\sin\left(3t + \frac{\pi}{4}\right)$

частота дискретизации?

Ответ: 6

$3 \cdot 2 = 6$

$y(t) = 2\sin\left(3t + \frac{\pi}{2}\right)$

3 - частота
2 - амплитуда
$3 \cdot 2 = 6$
угловая частота

$\omega_0 = \frac{2\pi}{T}$

$f = \frac{1}{T}$

$f = 2\left(\frac{\omega_0}{2\pi}\right) = \frac{6}{\pi}$

(Hz)

3,14159265

$y(t) = 2\cos(10t + \frac{\pi}{4}) + 2\sin(5t + \frac{\pi}{2})$

$f = \frac{\omega_0}{2\pi}$

$\frac{2\pi}{\omega_0} = T = \frac{1}{n}$

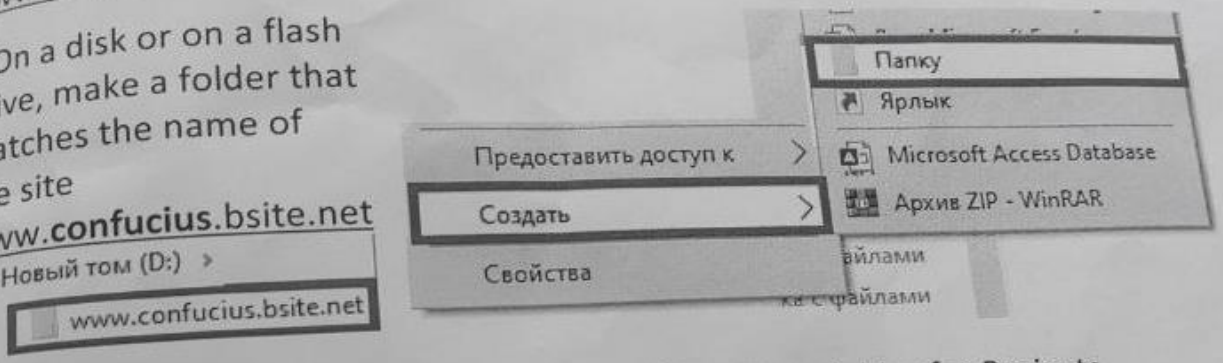
$f = \frac{\omega_0}{n} = \frac{10}{\pi} = 3,1$

What should you do in class:

0. Come up with a good name for your site.

I came up with a name for my site - Confucius (in my opinion, this is a good name)
www.**confucius**.bsite.net

1.On a disk or on a flash drive, make a folder that matches the name of the site
www.**confucius**.bsite.net



2. In a folder **D:\www.confucius.bsite.net** create a folder for Projects
D:\www.confucius.bsite.net\Projects

3. In a folder **D:\www.confucius.bsite.net\Projects** create a folder for Projects Number 0
D:\www.confucius.bsite.net\Projects\0

4. In a folder **D:\www.confucius.bsite.net\Projects\0** create file ***index.htm***

É. Galois (1811-1832) **Les Misérables | Do You Hear the People Sing?**

Example

There are $6!$ ways to order the letters of GALOIS

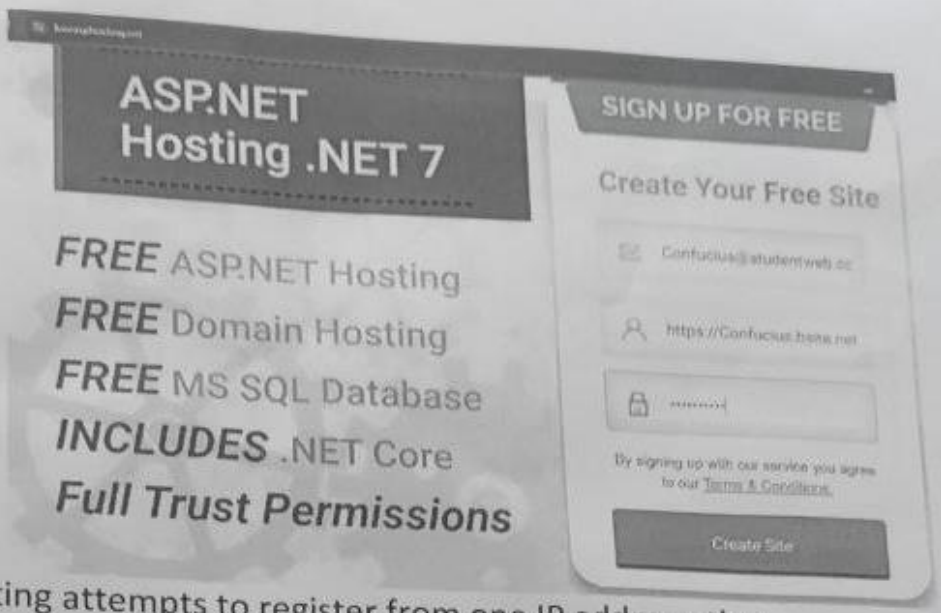
If randomly reorder the letters what is probability that the vowels (A, O, I) are all before consonants (G, L, S)? $= \frac{3}{6} \cdot \frac{2}{5} \cdot \frac{1}{4} = \frac{1}{20}$

$$\frac{3! \cdot 3!}{6!} = \frac{1}{20}$$

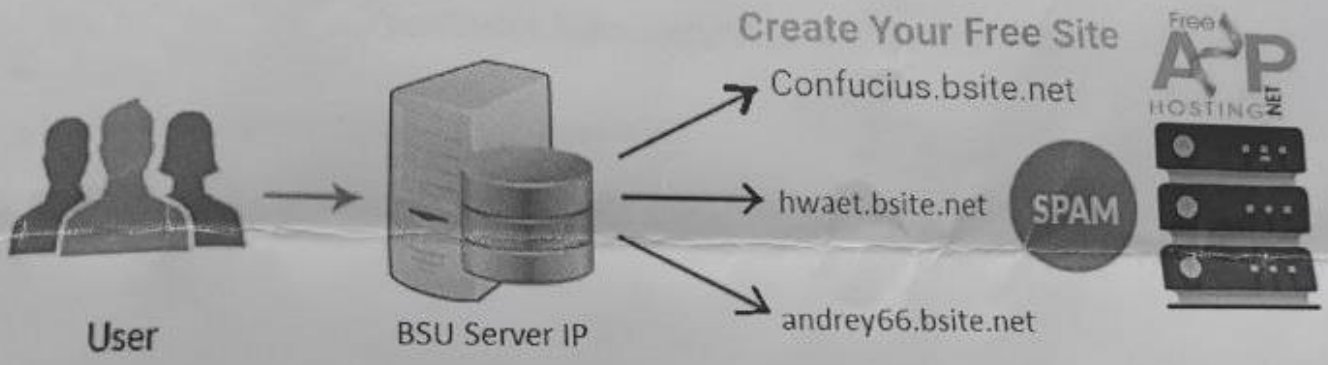
$$y_H = 2\cos\left(10t + \frac{\pi}{4}\right) + 2\sin\left(5t + \frac{\pi}{2}\right)$$

$$S_K = \frac{\omega^\circ}{h} = \frac{10}{4} = 3,1$$

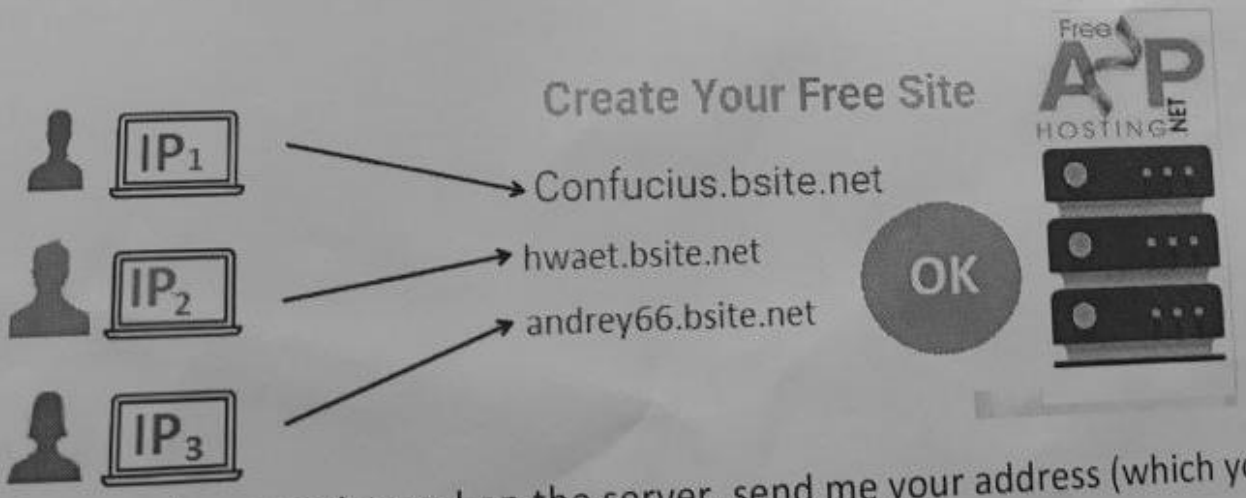
What should you do at home:
Register free hosting on **freeasphosting.net** At home because many hosting services do not register from one IP address.



If several dozen hosting attempts to register from one IP address, the **freeaspohosting.net** server may decide that this is a SPAMer and block it.



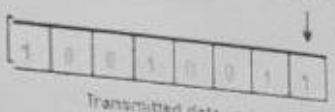
And if registration is carried out from different computers (with different IP addresses), then the freeasphosting.net server does not raise any suspicions.

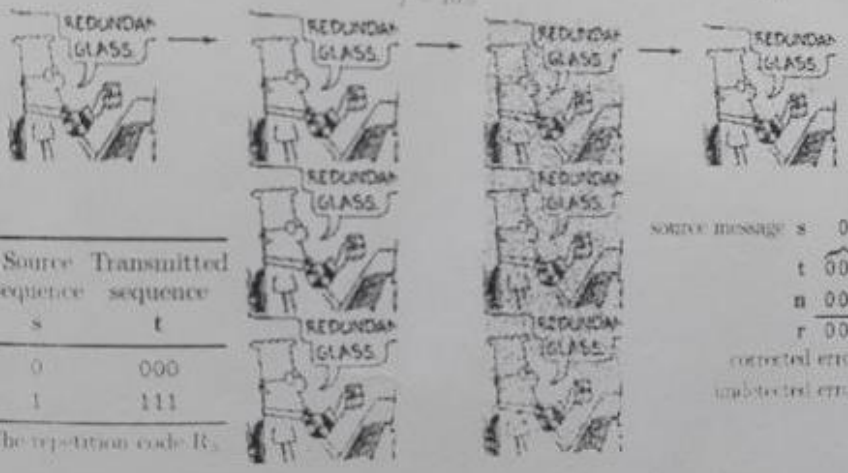


After you have registered on the server, send me your address (which you received during registration) by email.

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

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





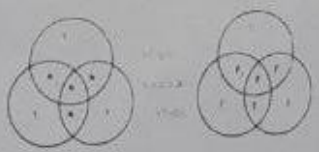
Source sequence s	Transmitted sequence t
0	000
1	111

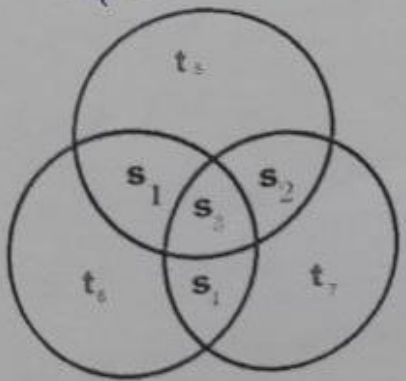
The repetition code R_3

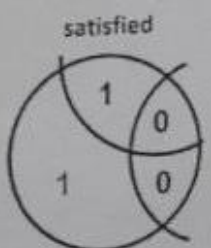
source message s	0	0	1	0	1	1	0
t	000	000	111	000	111	111	000
n	000	001	000	000	101	000	000
r	000	001	111	000	010	111	000
corrected errors		*					
uncorrected errors							*

7.4. Hamming code.

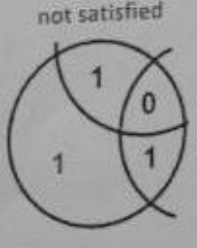
$$\frac{4}{7} \rightarrow \frac{7}{4}$$



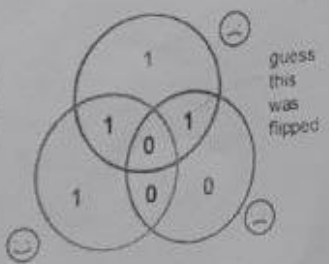




1+1+0+0=0



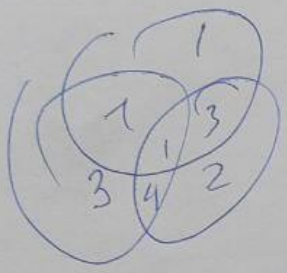
1+1+0+1=1



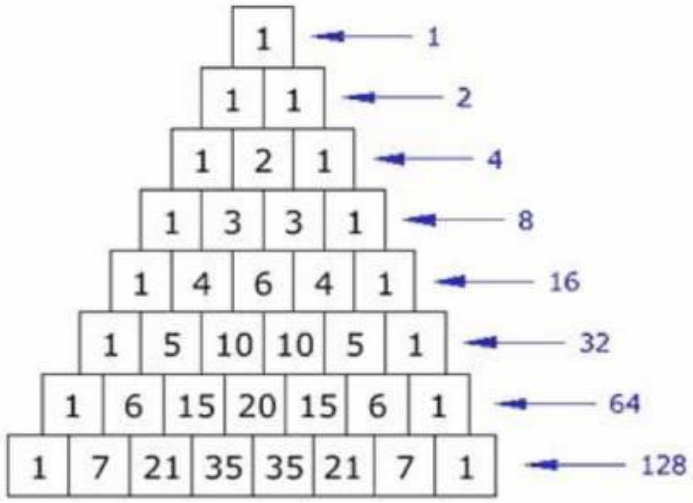
Чет 1->0

Нечет 1->1

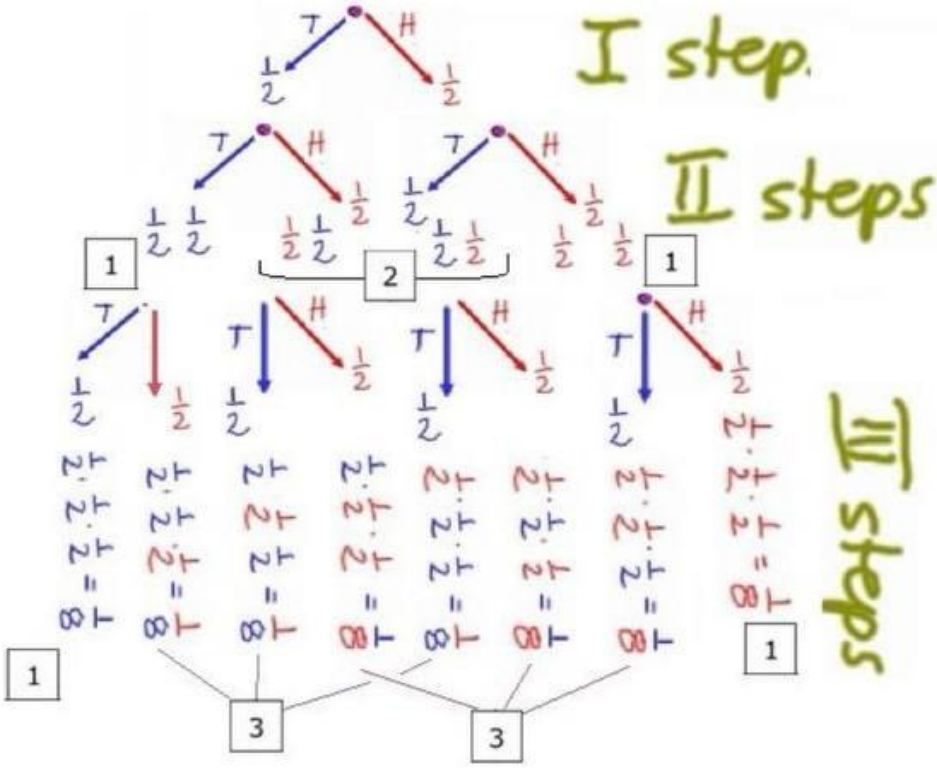
10001101



$$E = \sum_{i=0}^{n} \log x_i \log\left(\frac{1}{x}\right)$$ - формула энтропии



Pascal's triangle



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

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

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

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

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

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

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


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

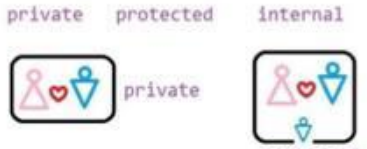
```
static void Main(string[] args)
 {
     Dog dori = new Dog();  //Constructor works
     dori.age = 3;

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

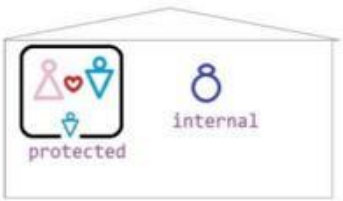
```
public Dog()
 {
 }
 public Dog(string name)
 {
     this.name = name;
 }
 public Dog(string name, string breed)
 {
     this.name = name;
     this.breed = breed;
 }
```

1 - **constructor** no returns value

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

3. more than one **constructor**






```
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

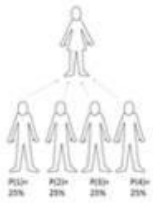
ASon.dll

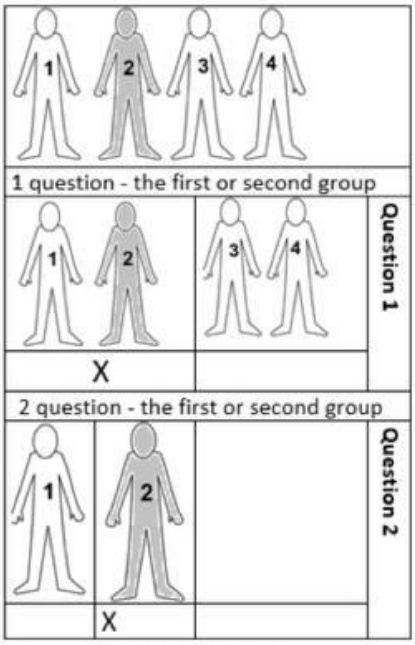
```
class ASon:AFather
{
    public ASon(string name)
    {
        base.name = name;
        base.age = 33;
    }
}
```

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





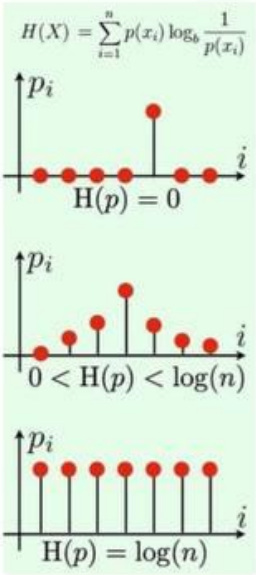
Average number of questions =

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**



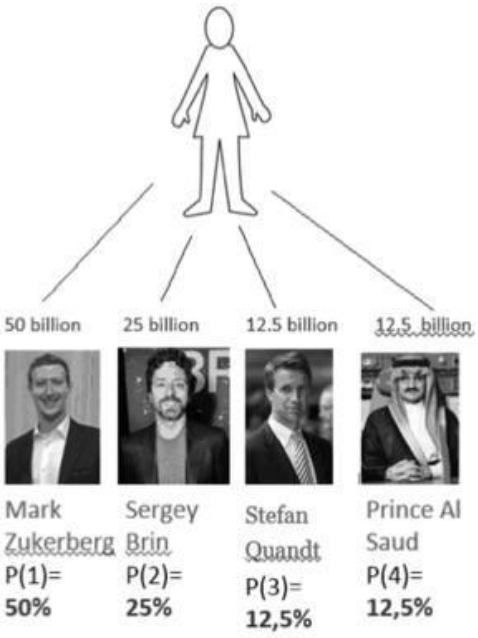
$$\sum_{i=1}^{n} p(i) \log_2 \frac{1}{p(i)}$$

Quantifying information

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

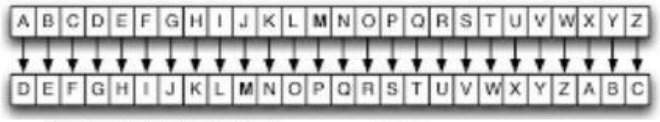
number of bits required to encode choice

$$\sum_{i=1}^{n} p(x_i)\, I(x_i)$$



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**

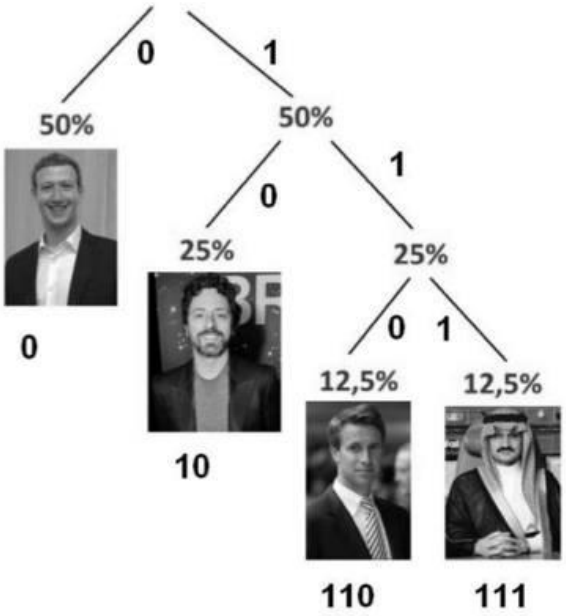
Frequency Analysis https://www.youtube.com/watch?v=sMOZf4GN3oc Khan

- 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.



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

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

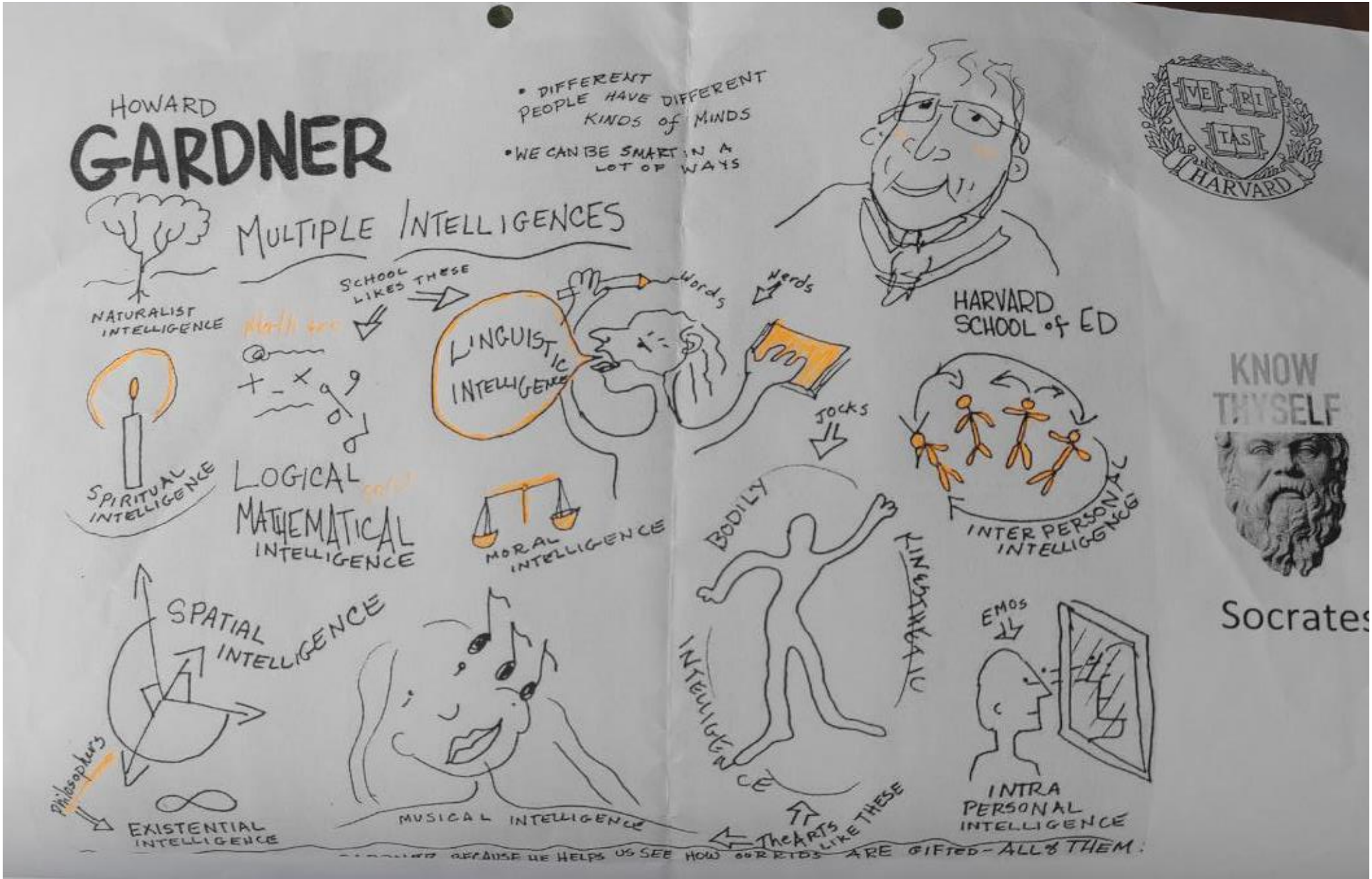
9

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

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


HOWARD
GARDNER
• DIFFERENT PEOPLE HAVE DIFFERENT KINDS of MINDS
• WE CAN BE SMART IN A LOT OF WAYS
MULTIPLE INTELLIGENCES
VE RI TAS
HARVARD
NATURALIST INTELLIGENCE
SCHOOL LIKES THESE
Words
Nerds
LINGUISTIC INTELLIGENCE
HARVARD SCHOOL of ED
KNOW THYSELF
SPIRITUAL INTELLIGENCE
LOGICAL MATHEMATICAL INTELLIGENCE
MORAL INTELLIGENCE
JOCKS
BODILY KINESTHETIC INTELLIGENCE
INTER PERSONAL INTELLIGENCE
Socrates
SPATIAL INTELLIGENCE
EMOS
Philosophers
EXISTENTIAL INTELLIGENCE
MUSICAL INTELLIGENCE
The ARTS LIKE THESE
INTRA PERSONAL INTELLIGENCE
ARE GIFTED - ALL 8 THEM.