

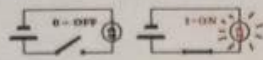
Handwritten signature



Massachusetts Institute of Technology (MIT)



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



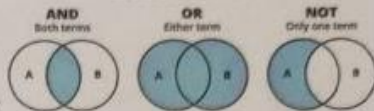
Logical addition
(disjunction)

A	B	$F = A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

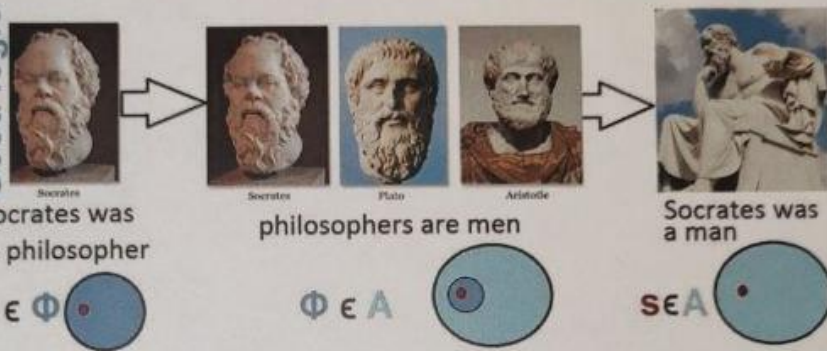
A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False



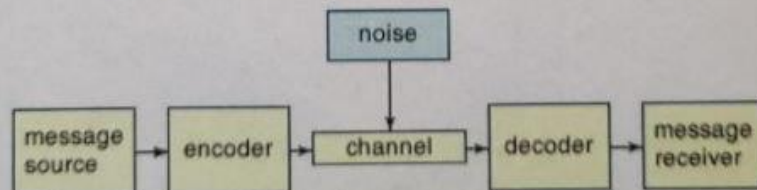
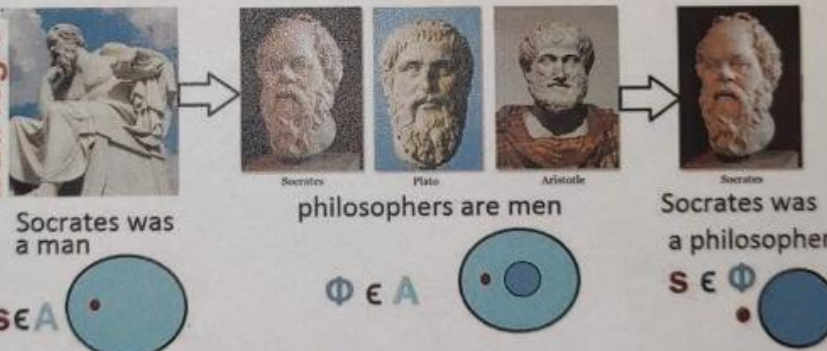
BOOLEAN LOGIC



Good logic



Bad logic



© 2000 Encyclopædia Britannica, Inc.

Resume of Lecture by Pr. Bob Gallagher from MIT Massachusetts Institute of Technology (MIT)

George Boole (1815-1864) developed Boolean logic.

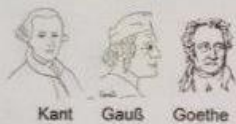
The principles of logical thinking have been understood (and occasionally used) since the Hellenic era.

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 contribution 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.

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



Kant

Gauß

Goethe

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)


The Mathematical Theory of Communication



Creating a reliable connection over an unreliable (noisy) channel that's what IT is about

and that's what Shannon did





Walking in Oxford on a cold and rainy day
 With prof. Matthias Winkel

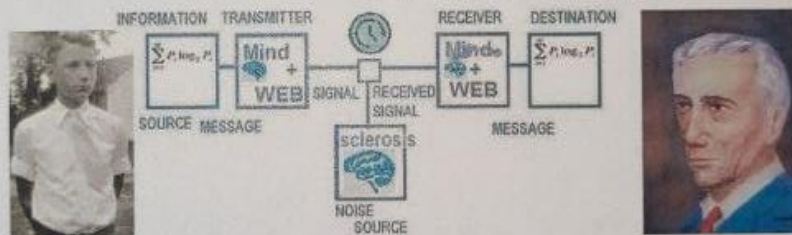
Markoff Chain Probability Model for Oxford Weather:



CHALK + TALK **ink + think**



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



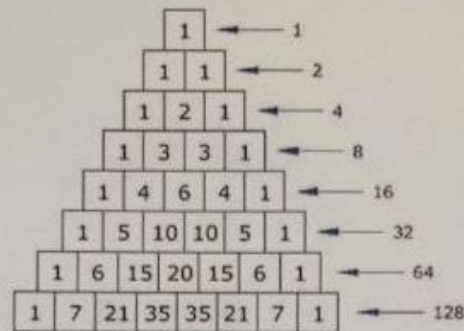
School \rightarrow ~~formalism~~ \Rightarrow University \Rightarrow ~~formalism~~ \Rightarrow ~~formalism~~

Motivation: 80% chance of rain
 Let A_i be the event of rain at Jan on day i of this term, $1 \leq i \leq n$
 Suppose the events A_i are independent.

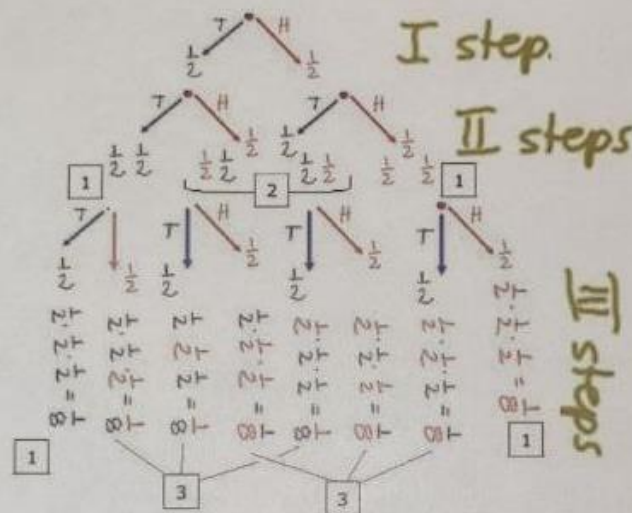
Oxford

Day	Temp	Wind	Humidity	Rain
Tue 13th	10°	10%	10%	10%
Wed 14th	13°	10%	10%	10%
Thu 15th	13°	10%	10%	10%
Fri 16th	11°	10%	10%	10%

then take notes on the lecture yourself



Pascal's triangle

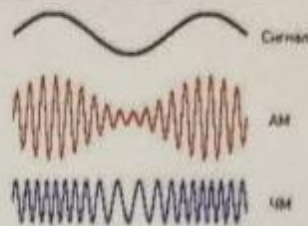


$$\begin{aligned}
 (a + b)^0 &= 1 \\
 (a + b)^1 &= a + b \\
 (a + b)^2 &= a^2 + 2ab + b^2 \\
 (a + b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\
 (a + b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
 (a + b)^5 &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5
 \end{aligned}$$

Handwritten signature or scribble in the top left corner.



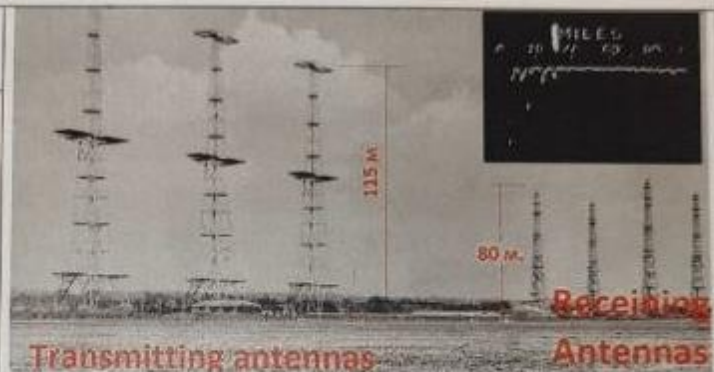
Reginald A. Fessenden
(October 6, 1866 – July 22, 1932)



(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.

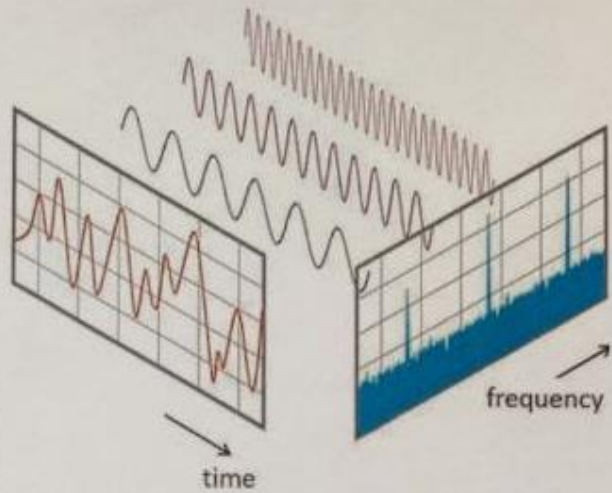


Ralph Hartley
(81:1888-1970)

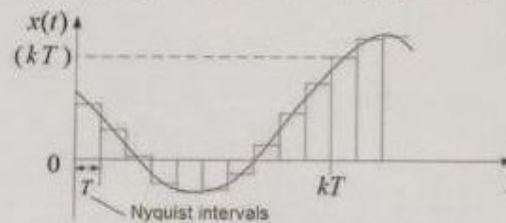
$$H = n \log s$$

$$= \log s^n.$$

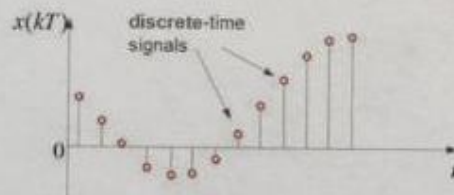
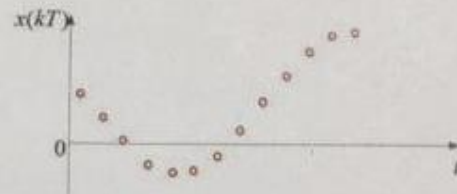
Fourier transform



Sampling. Kotelnikov-Nyquist Theorem

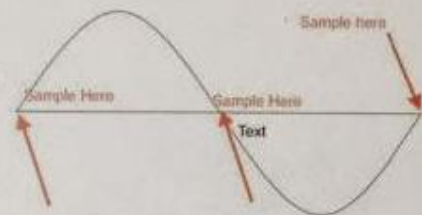


Time intervals T , through which readings $s(kT)$ are taken, are called Nyquist intervals.



Sine with period T

Sampling at $T/2$



frequency Sample



$$F_{\text{sample}} \geq 2 * F_{\text{max}}$$

$$(T_{\text{sample}} \leq T_{\text{min}}/2)$$

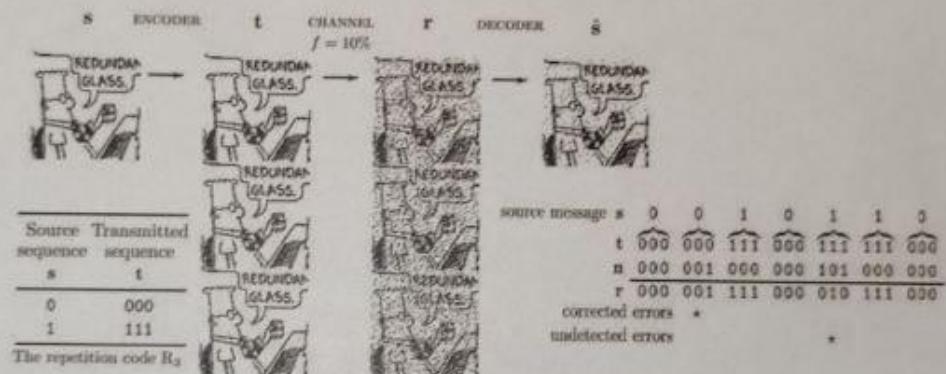
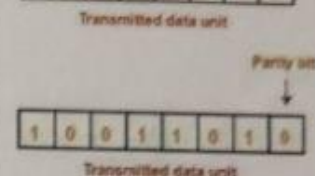
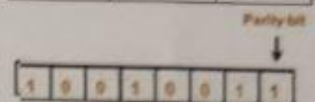
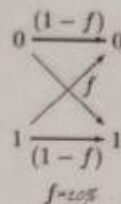
Cancer



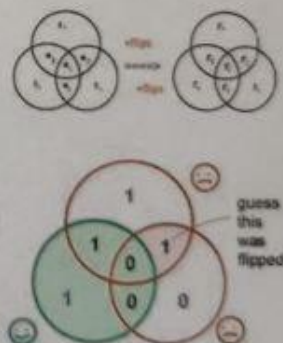
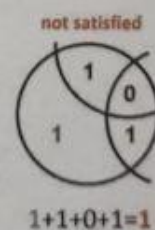
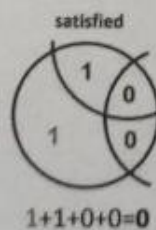
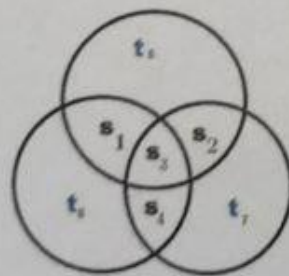
Sir Dr. D. MacKay,
University of Cambridge
(22 April 1967 – 14 April 2016)



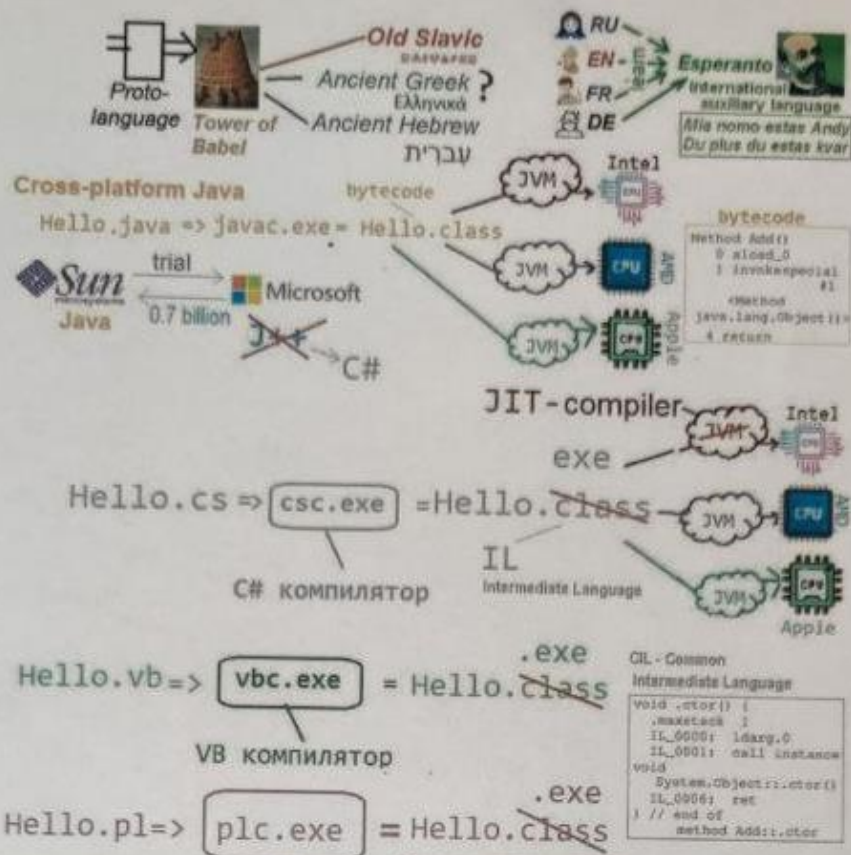
"I believe in clean energy,
but I also believe in mathematics"



7.4. Hamming code. $\frac{4}{\Sigma} \rightarrow \frac{7}{t}$



C#



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)

CH 2. Colanar

```
class Dog
{
```

```
    public string name;
    public string breed;
    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



public

private protected internal



private protected

internal



private protected

```
class AFather
```

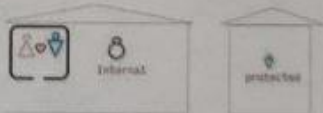
```
{
    protected string name;
    int age;
}
class ASon:AFather
{
    public ASon(string name)
    {
        base.age = 33;
        base.name = name;
    }
}
```

```
class Program
```

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

```
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");
    }
}
```

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



internal

protected

Busq xenuxa



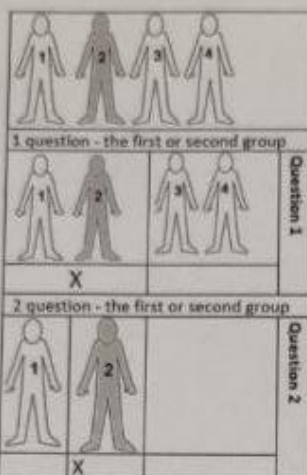
Say **NO** to the first



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 = $2 \cdot 0.25 + 2 \cdot 0.25 + 2 \cdot 0.25 + 2 \cdot 0.25 = 2$

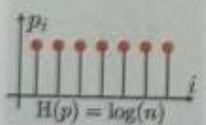
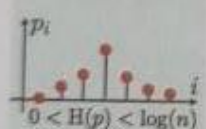
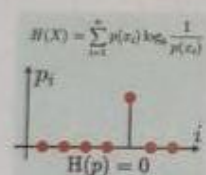
Average number of questions =

$$1 \cdot 0.5 + 2 \cdot 0.25 + 3 \cdot 0.125 + 3 \cdot 0.125$$



Question 1. Is this Zuckerberg?	 50%	$1 \cdot 0.5$
Question 2. Is this Sergey Brin?	 25%	$2 \cdot 0.25$
Question 3. Is this Stefan from BMW?	 12.5%	$3 \cdot 0.125$
So Prince Saud	 12.5%	$3 \cdot 0.125$

Average number of questions = 1.75



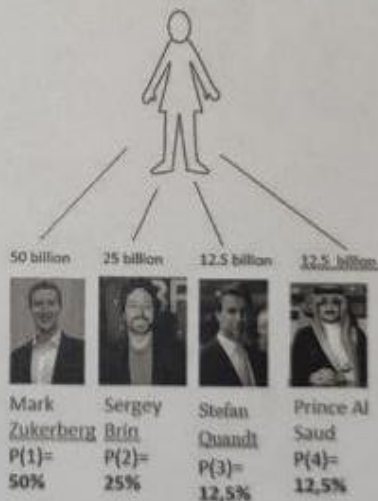
$$\sum_{i=1}^n p(i) \log_2 \frac{1}{p(i)}$$

Quantifying information

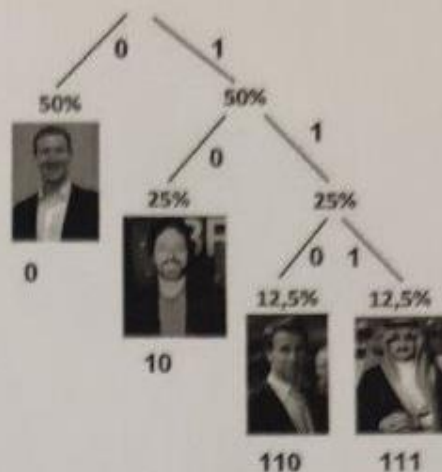
$$I(x_i) = \log_2 \left(\frac{1}{p_i} \right)$$

number of bits required to encode choice

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



Toxe



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

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

ла мама 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
ар - 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 (diagram (2-symbols) structure as in Belarusian)



Caesar Cipher

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

2. We can also create the same cipher. If we add 3 to every number, we might use this key:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

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

Plaintext	A	B	B	A
Ordinal/Position	1	2	2	1
Keyword (LEW)	L	E	W	L
Keyword Ordinal/Position	12	5	23	12
Sum	13	7	25	13
Ciphertext	M	G	X	M

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 rotating a keyword.

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

Source: <https://www.youtube.com/watch?v=8dHd0f0d0d0>

Frequency Analysis

- 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 1 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%	4.2%	12.7%	2.1%	2.0%	6.9%	13.3%	0.9%	2.4%	4.0%	4.4%
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.7%	7.7%	1.9%	0.1%	6.0%	4.1%	9.1%	2.2%	0.8%	2.3%	0.4%	0.1%	1.1%

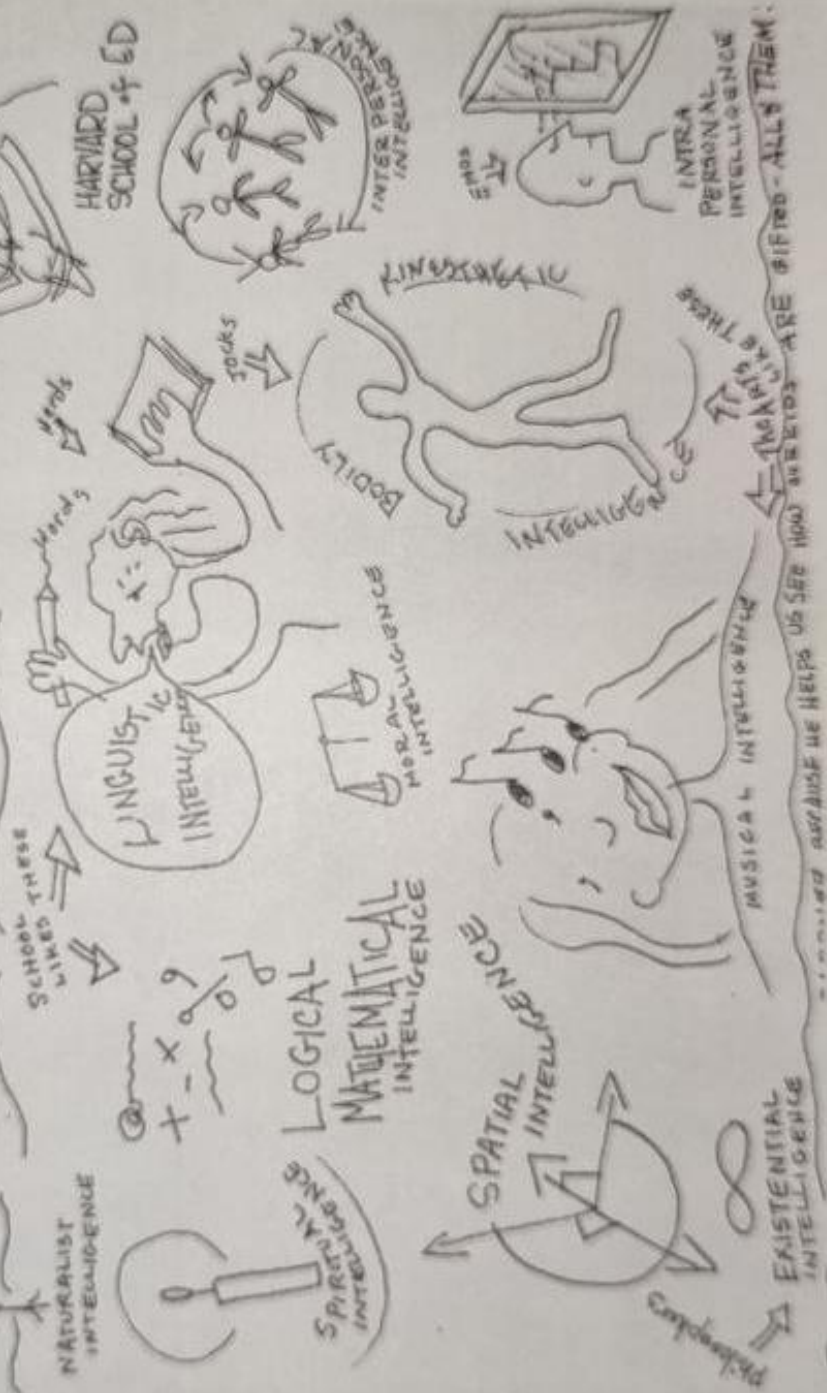
- Some letters appear very frequently, such as E or T and some letters appear very infrequently, such as J or K. Using these frequencies, we can look at what appears frequently or infrequently in the cipher-text and perhaps find certain patterns.
- While it's human it might be tedious to conduct frequency analysis to decode a message, a computer can do it very quickly.

HOWARD

GARDNER

MULTIPLE INTELLIGENCES

- * DIFFERENT PEOPLE HAVE DIFFERENT KINDS OF MINDS
- * WE CAN BE SMART IN A LOT OF WAYS



HARVARD SCHOOL 4-ED



KNOW
YOURSELF



Socrates