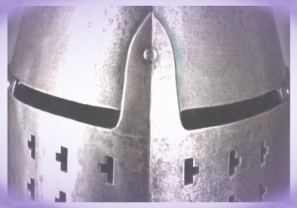
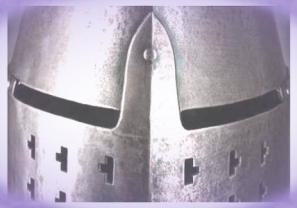


Cryptography and Network Security

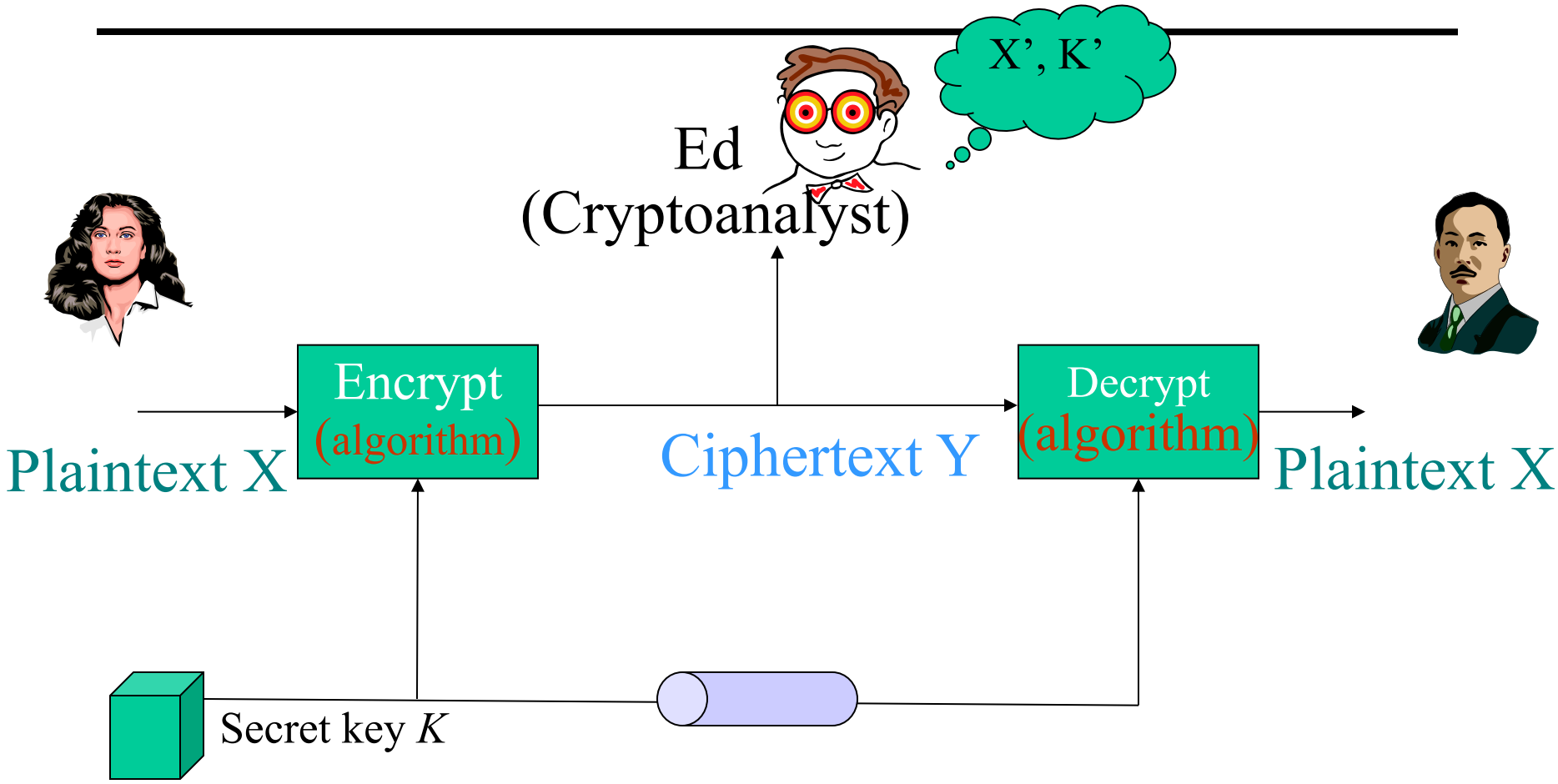
Eighth Edition
by William Stallings



Chapter 3

Classical Encryption Techniques

Classical Cryptography – Possible Attacks



Discussion: How to attack Cæsar cipher?

Let k = 9, m = "VELVET" (21 4 11 21 4 19)

$E_k(m)$ = (21+9 4+9 11+9 21+9 4+9 19+9) mod 26

= (30 13 20 30 13 28) mod 26

="4 13 20 4 13 2" = "ENUENC"

$D_k(m)$ = (26 + c – k) mod 26

= (21 30 37 21 30 19) mod 26

= "21 4 11 21 4 19" = "VELVET"

Attacks

- Opponent whose goal is to break cryptosystem is the *adversary*
- Three types of attacks:
  - ***ciphertext only***: adversary has only ciphertext; goal is to find plaintext, possibly key
  - ***known plaintext***: adversary has ciphertext, corresponding plaintext; goal is to find the key
  - ***chosen plaintext***: adversary may supply plaintexts and obtain corresponding ciphertext; goal is to find key

Attacking a conventional cryptosystem

- Cryptoanalysis:
  - Art/Science of breaking an encryption scheme
  - Exploits the characteristics of algorithm/ mathematics
    - Recover plaintext from the ciphertext
    - Recover a key that can be used to break many ciphertexts
- Brute force
  - Tries all possible keys on a piece of ciphertext
    - If the *number of keys* is small, the adversary can get the correct key easily by simply trying!

Crack Caesar Cipher!

- example:

  Plaintext: ?

  Key : ?

  Ciphertext: `PHHW PH DIWHU WKH WRJD SDUWB`

- Try all possible keys: 0, 1, 2, … 25.
- It works when key=`3`: meaningful plaintext generated.
- We are done!

How about more complicated ciphers?

- Mono-alphabetic substitution cipher
  - Each plaintext letter is randomly assigned to its ciphertext letter.

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
q	a	z	w	s	x	e	d	c	r	f	v	t	g	b	y	h	n	u	j	m	i	k	o	l	p

  - How many possible ways of assignment?
    - 26!
    - Takes a looooong time to try every possible assignment.

Basis for Cryptoanalysis

- Mathematical attacks
  - Based on analysis of underlying mathematics
- Statistical attacks
  - Make assumptions about the distribution of letters, pairs of letters, triplets of letters, *etc.* (called models of the language).
  - Examine ciphertext, correlate properties with the assumptions.

Statistical Attacks Example

- Rail-Fence Cipher
  - Plaintext is `HELLO WORLD`
  - Rearrange as

    `HLOOL`

    `ELWRD`
  - Ciphertext is `HLOOL ELWRD`

Attacking the Cipher

- Anagramming
  - If 1-gram frequencies match English frequencies, but other *n*-gram frequencies do not,
  - Then probably a transposition
  - Rearrange letters to form *n*-grams with highest frequencies

Example

- Ciphertext: `HLOOLELWRD`
- Frequencies of 2-grams beginning with H
  - HE 0.0305
  - HO 0.0043
  - HL, HW, HR, HD < 0.0010
- Frequencies of 2-grams ending in H
  - WH 0.0026
  - EH, LH, OH, RH, DH ≤ 0.0002
- Implies E may follow H

Example

- Arrange so that H and E are adjacent

```
HE
LL
OW
OR
LD
```

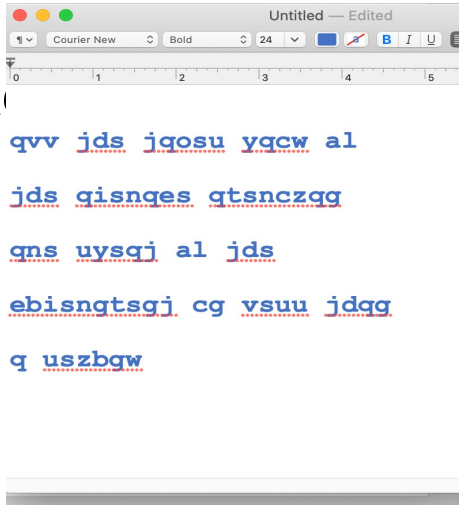
- Read off across, then down, to get original plaintext

Frequency Analysis – Hands on example

- Break this Ciphertext (known that it is generated by Mono-alphabetic substitution cipher):

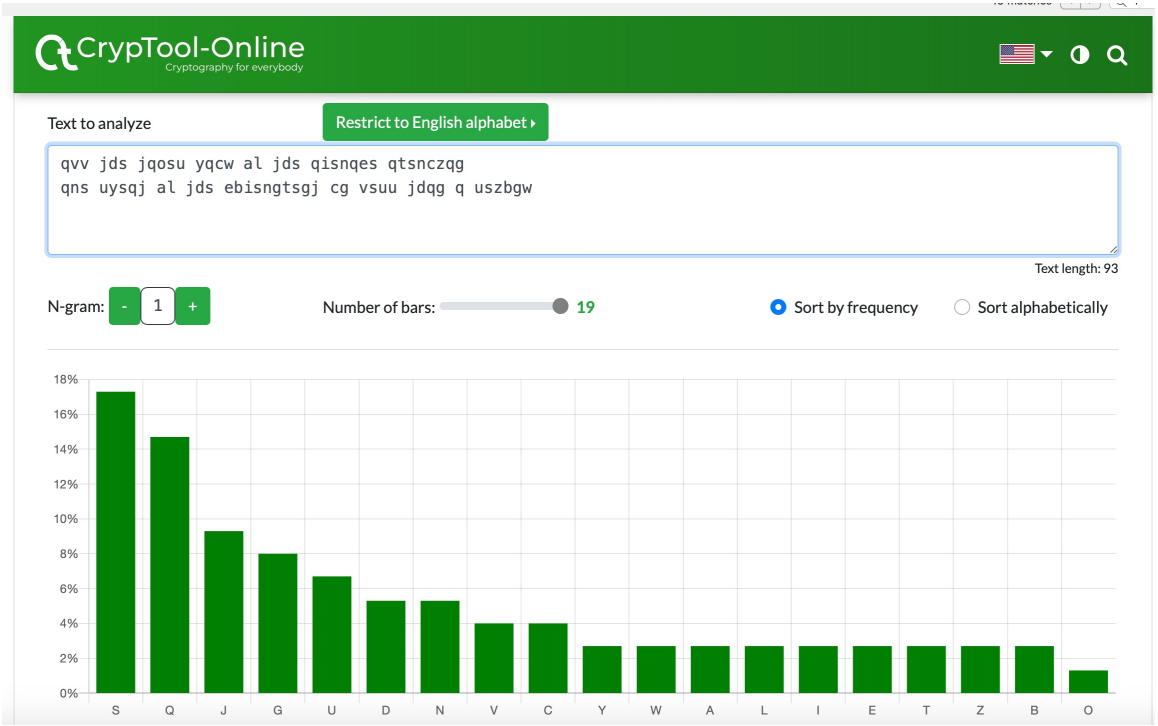
```
qvv jds jqosu yqcw al jds qisnqes
qtsnczqg qns uysgj al jds ebisngtsgj cg
vsuu jdqg q uszbgw
```

Step 0: copy the ciphertext into a blank .txt fil



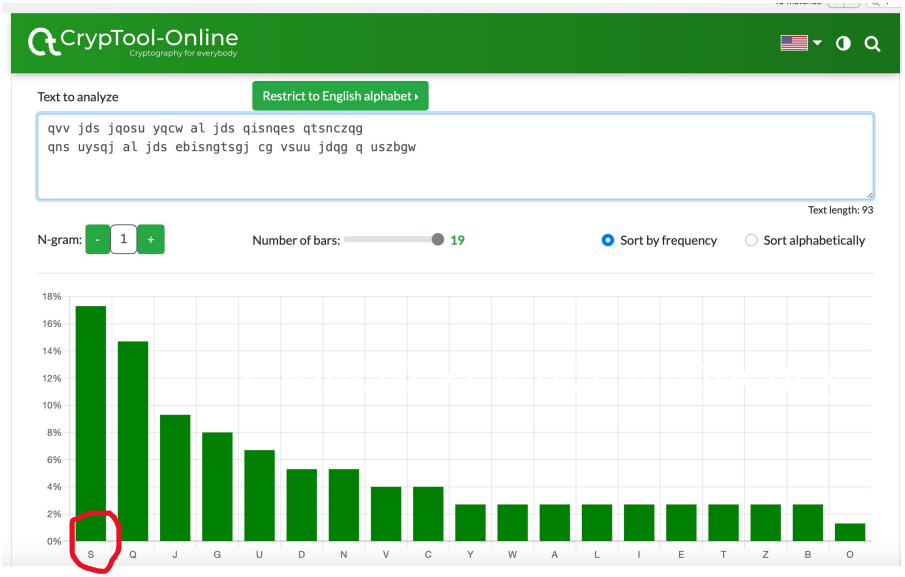
Hands on activities– frequency analysis

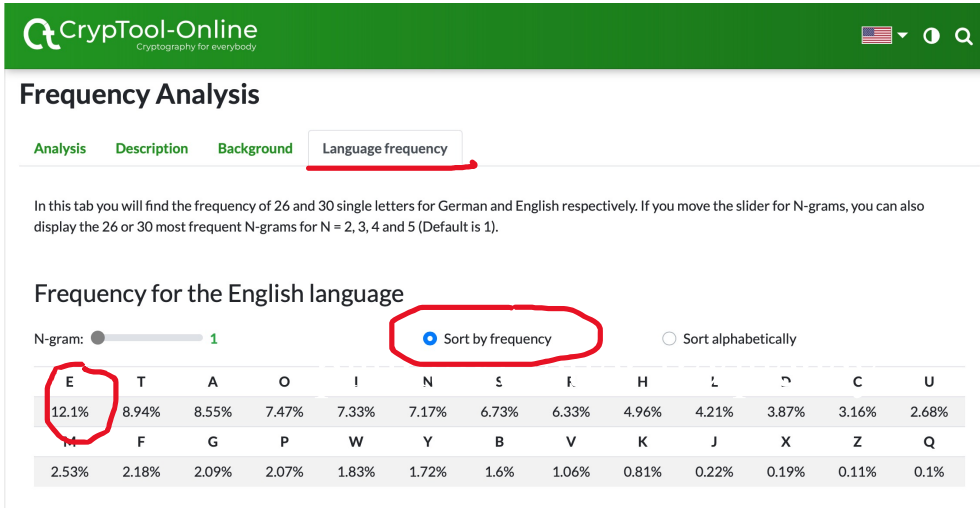
- Step 1: compute letter frequency
  - Copy the ciphertext into ” Text to analyze” on Cryptool https://www.cryptool.org/en/cto/frequency-analysis



Hands on activities – frequency analysis

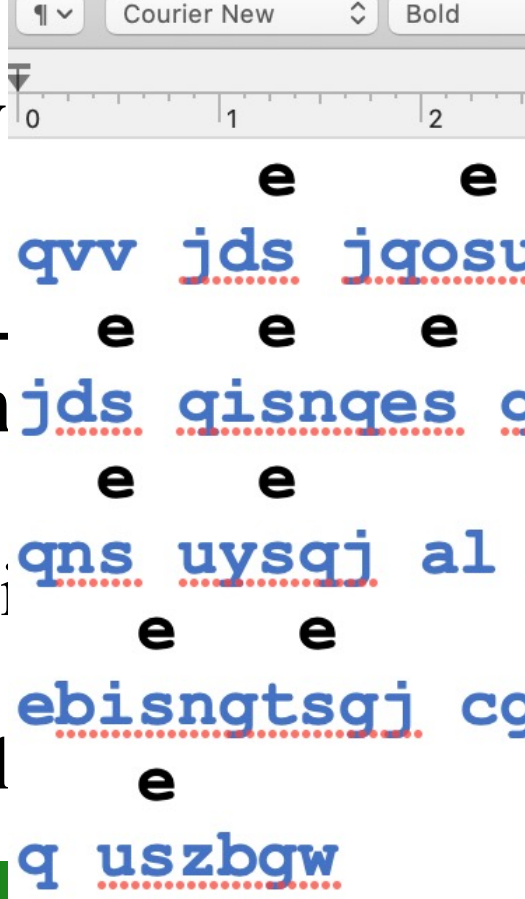
- Step 2: find the most frequent letter in ”Language frequency”
  - Guess ciphertext letter “**s**” is corresponding to plaintext letter “**e**”
  - write “e” on top of each “s” in the .txt file.

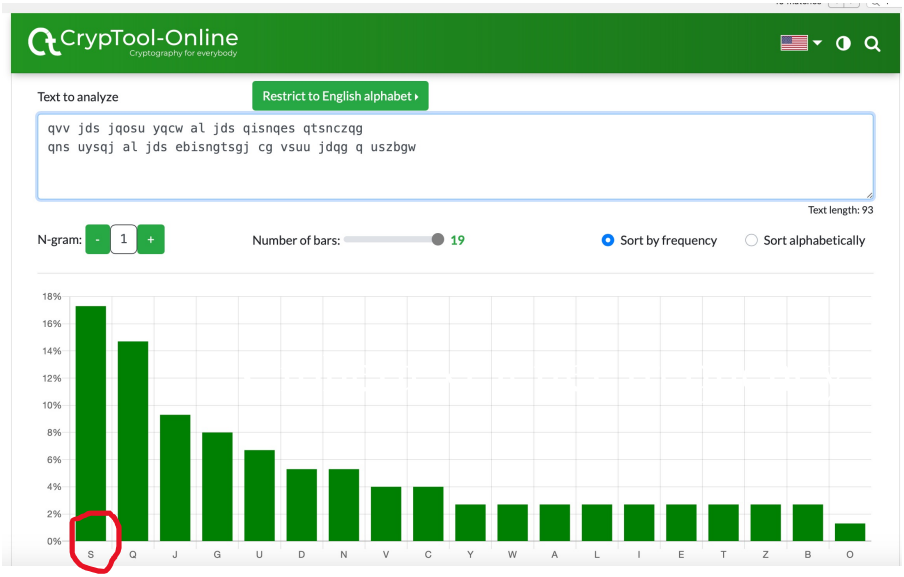


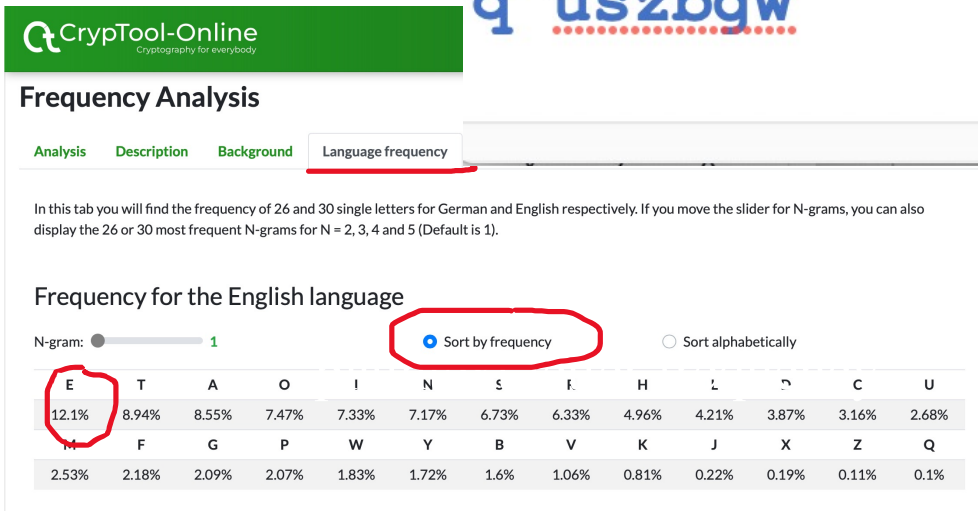


Hands on activities – frequency

- Step 2: find the most frequent letter in ”Language frequency”
  - Guess ciphertext letter “**s**” is correspondi plaintext letter “**e**”
  - write “e” on top of each “s” in the .txt fil

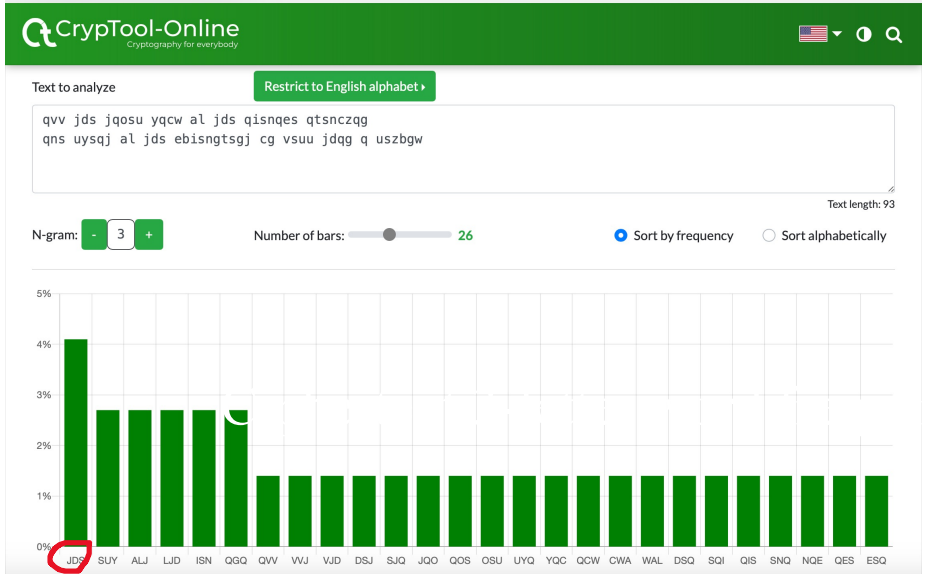


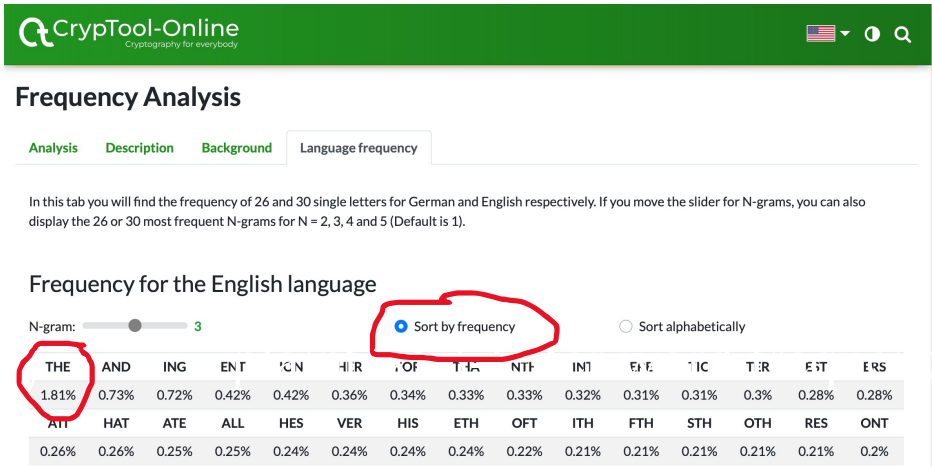




Hands on activities– frequency analysis

- Step 3: 3-letter word frequency
  - Set N-gram=3 in ciphertext analysis and in Language Frequency.
  - Guess ciphertext "___" is corresponding to plaintext word "the". (letter-to-letter)
  - Write plaintext letters on top of corresponding ciphertext in your .txt file.





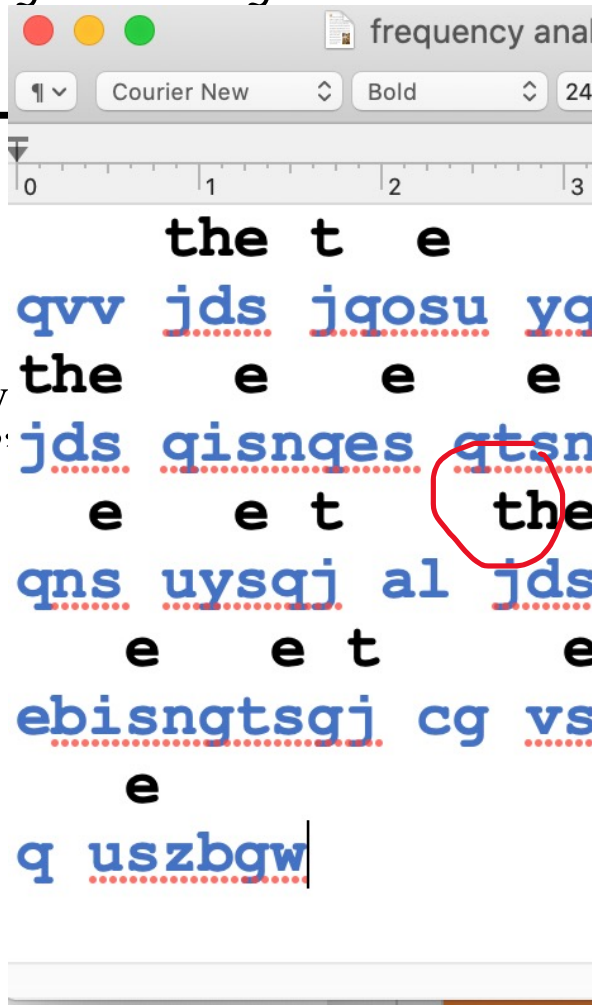
Hands on activities– frequency analysis

- Step 4: Form possible words and test.
  - Look at the ciphertext word "**jdqg**". It may be "this", "that", "than"…
  - Check the frequency of q in ciphertext, and compare with English. Which is more likely to be the plaintext of "q"? How about "g" in "jdqg"?
  - Test your guess by put them on top of each q and g in ciphertext.
  - What word could the first word "qvv" be?
  - After you guess/decode "v", what could "vsuu" be?

  - Continue to put your guess on top of corresponding ciphertexts and detect more words.
  - Remember to use frequency chart to help you.
  - Try to finish by yourself.

Hands on activities– frequency analysis

- Step 4: Form possible words and test.
  - Look at the ciphertext word "**jdqg**". It may be "this", "that", "than"…
  - Check the frequency of q in ciphertext, and compare w English. Which is more likely to be the plaintext of "q" How about "g" in "jdqg"?
  - Test your guess by put them on top of each q and g in ciphertext.
  - What word could the first word "qvv" be?
  - After you guess/decode "v", what could "vsuu" be?
  - Continue to put your guess on top of corresponding ciphertexts and detect more words.
  - Remember to use frequency chart to help you.
  - Try to finish by yourself.



Attacking the Vigenere Cipher

- Approach
  - Establish period; call it n
  - Break message into n parts, each part being enciphered using the same key letter
  - Solve each part
- We will show each step

```
key       VIGVIGVIGVIGVIGV
plain     THEBOYHASTHEBALL
Cipher    OPKWWECIYOPKWIRG
```

The Target Cipher

- We want to break this cipher:

```
ADQYS MIUSB OXKKT MIBHK IZOOO
EQOOG IFBAG KAUMF VVTAA CIDTW
MOCIO EQOOG BMBFV ZGGWP CIEKQ
HSNEW VECNE DLAAV RWKXS VNSVP
HCEUT QOIOF MEGJS WTPCH AJMOC
HIUIX
```

First Tool: Kaskski's Method

- Kaskski: if characters of the key appear over the same characters in the plaintext, repetitions in the ciphertext will occur

```
key       VIGVIGVIGVIGVIGV
plain     THEBOYHASTHEBALL
cipher    OPKWWECIYOPKWIRG
```

  - Distance between repetitions is 9, so the period must be a factor of 9 (that is, 1, 3, or 9)
  - Will the ciphertext contain the same repetition in the following two cases?

```
key     VIGVIGVIGVIGVIGVI      key     VIGJVIGJVIGJVIGJ
plain   THEBOOYHASTHEBALL      plain   THEBOYHASTHEBALL
```

Repetitions in Example

Letters	*Start*	*End*	*Distance*	*Prime Factors*
MI	5	15	10	2, 5
OO	22	27	5	5
OEQOOG	24	54	30	2, 3, 5
FV	39	63	24	2, 2, 2, 3
AA	43	87	44	2, 2, 11
MOC	50	122	72	2, 2, 2, 3, 3
QO	56	105	49	7, 7
PC	69	117	48	2, 2, 2, 2, 3
NE	77	83	6	2, 3
SV	94	97	3	3
CH	118	124	6	2, 3

Estimate of Period

- The longest repetition *OEQOOG* is probably not a coincidence
  - Distance is 30
- The second longest is *MOC*
  - Distance is 72
- GCD of 30 and 72 is 6
- Others
  - (7/10) have 2 in their factors
  - (6/10) have 3 in their factors
- 6 is a probable period

Summary

- Explain how to crack Ceaser cipher using the brute force attack
- Explain how to crack Rail-Fence cipher using Cryptoanalysis
- Explain how to crack Mono-alphabetic cipher using Frequency analysis

- Explain how to crack Vegenere cipher