Name: _____ **Student No.:** _____ **Date:** __/__/____

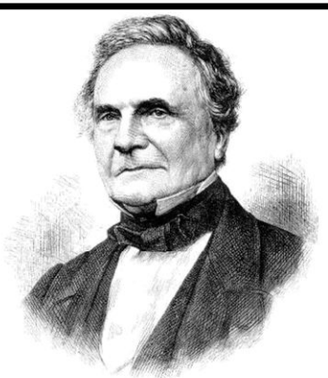
Cryptanalysis

KASISKI EXAMINATION

It is method to break **polyalphabetic substitution ciphers** such as the Vigenère cipher.

In the Vigenère cipher, **the key is repeated**, which **can cause repeating sequences** in the ciphertext.

This method finds these repeating sequences **to help determine the key length.**



Friedrich Kasiski

Directions: Crack the code and guess the song!

The ciphertext given to you in Google Classroom contains **lyrics from a song** by one of Billboard's **25 greatest pop stars of the 21st century.**

The message was encrypted using the **Vigenère cipher** with a **4-letter key**, which is the **artist's code** from the list below:

Artist	Code	Artist	Code	Artist	Code
Adele	ADLE	**Eminem**	EMNM	**Nicki Minaj**	NKMJ
Ariana Grande	ARGR	**Jay-Z**	JAYZ	**One Direction**	ONDR
Bad Bunny	BDBY	**Justin Bieber**	JBIB	**Rihanna**	RIHN
Beyoncé	BEYC	**Justin Timberlake**	JTBK	**Shakira**	SHKR
Britney Spears	BRSP	**Kanye West**	KAWT	**Taylor Swift**	TSWF
Bruno Mars	BRMS	**Katy Perry**	KTPY	**The Weeknd**	TWKD
BTS	BTSX	**Lady Gaga**	LGGA	**Usher**	USHR
Drake	DRKE	**Lil Wayne**	LIWN		
Ed Sheeran	EDSH	**Miley Cyrus**	MYCY		

In this worksheet, we'll first **verify that the key length used is indeed 4**, then we'll **use frequency analysis to help determine the actual key.**

Step 1: Get your ciphertext from Google Classroom. **Write it down clearly.**

Example:

FZCTZAFGSI GO MSMMJR LQX
MK UVVPQVRBGE FW APYP GNFPCDI
ZCCC G EBR QGFCMWS LYNP
CMW LRMY ZSSTF QW UBZGP HVYEF
CMWSI CXFVWVIMLI J RCGE ELF NSPG
JXQ YSMRVFR YNM STGS CMWS JYEF
FYDZ M ACO JCGM CMWS LYNP
TPCZ MR YPRR HBHC CXEW
K DEL HFIJ APYP JBPM JBPM JBPM
K DEL UFI WQVV FCMS FCMS FCMS

Step 2: Scan the QR code to access the **online Kasiski Examination tool.**

Step 3: Paste your ciphertext in the **"Intercept" box** and **click "Find Repeated Sequences".**

A **table of repeated sequences** will appear below.

Example:

- The **first column** lists the **repeated sequences.**
- The **second column** represents the **distances between occurrences of these repeated sequences.**
- The **remaining columns** contain the **factors of each respective distance.**

		2	3	4	5	6	7	8
FCMW	32	Y		Y				Y
CMWS	76	Y		Y				
MWSL	96	Y	Y	Y		Y		Y
APYP	152	Y		Y				Y
BPMJ	4	Y		Y				

Step 4: Find five unique repeated sequences with **different distances.**

Step 5: Find the factors of each distance.

You can use an online Factoring Calculator.

Example:

Repeated Sequence	Distance	Factors
FCMW	32	1, 2, 4, 8, 16, 32
CMWS	76	1, 2, 4, 19, 38, 76
MSWL	96	1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96
APYP	152	1, 2, 4, 8, 19, 38, 76, 152
JBPM	4	1, 2, 4

Repeated Sequence	Distance	Factors

Step 6: Check the first repeated sequence in your table.

In your ciphertext above, **use boxes to find the repeated sequence** where the distance between the first letters of the first and second occurrences **matches the distance shown in the tool.**

Example:

- **The first repeated sequence in the table is "FCMW"**
- **Check the ciphertext you have written.**
- **Starting from the letter after the first occurrence of "FCMW", there are 32 letters to reach the first letter of the next "FCMW".**

Step 7: Check all the common factors in your table.

✓ What common factors did you find?

_____

✓ Based on the common factors, is it possible that the key length is 4?

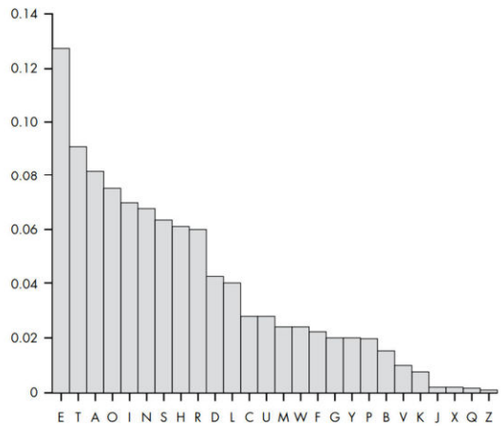
☐ YES

☐ NO

FREQUENCY ANALYSIS

It is a method used to break substitution ciphers by **counting how often each letter appears in the text.**

The **most frequent letters in the ciphertext** are assumed to **match the most common letters in English (E, T, A, O, I, and N).**



Now, let's find your 4-letter key!

Step 7: In the **"Finding the Key"** of the Kasiski Examination tool, **set the "Keyword Length" to 4.**

Step 8: In **"Keyword Letters", L1 to L4** represent **first to fourth subkeys.**

Step 9: Click "L1" (first subkey), and **two bar graphs will appear:**

- **Red** graph shows **letter frequencies in English alphabet.**
- **Blue** graph shows **letter frequencies from your ciphertext by examining every fourth letter, starting from the first letter.**

Step 10: Adjust the "Shift" value until **the blue graph pattern looks similar to the red graph.**

- You can try **shifting the most frequent letter in your ciphertext to "E"** to find a possible key, though **it doesn't always work.**
- **Finding the right key is a trial-and-error process.**

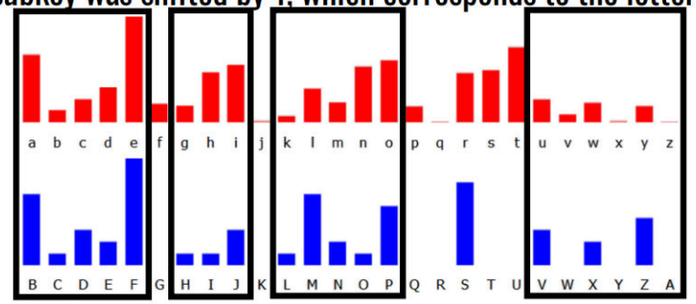
Step 11: Repeat Steps 9 and 10 for "L2", "L3", and "L4".

Step 12: Screenshot, print, and paste the letter frequencies in each box.

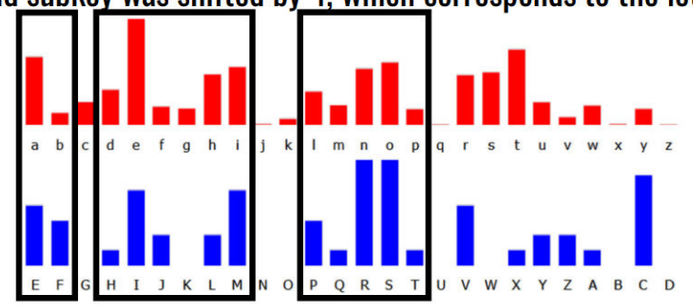
Step 13: For each subkey, **draw a box around the area** where the **blue and red graph trends look similar after shifting.**

Example:

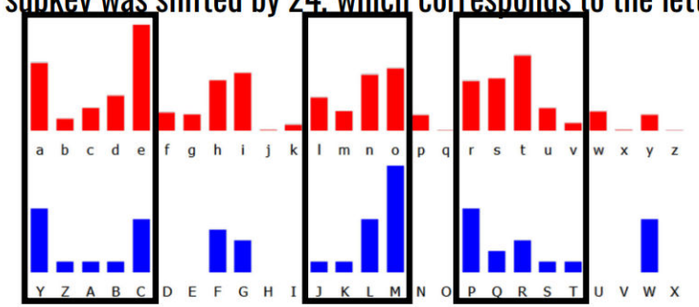
- The first subkey was shifted by 1, which corresponds to the letter "B".



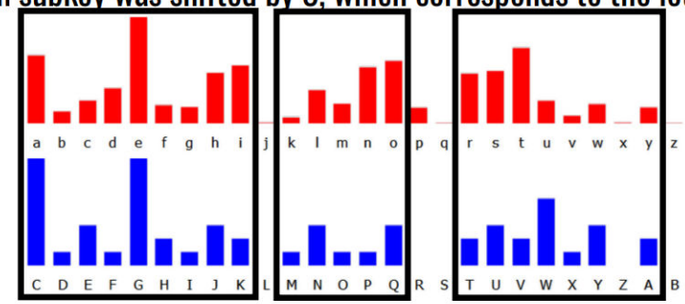
- The second subkey was shifted by 4, which corresponds to the letter "E".



- The third subkey was shifted by 24, which corresponds to the letter "Y".



- The fourth subkey was shifted by 3, which corresponds to the letter "Y".



✓ **First subkey letter: ____**

✓ **Second subkey letter: ____**

✓ **Third subkey letter: ____**

✓ **Fourth subkey letter: ____**

✓ **What is your Vigenère key?**

____ ____ ____ ____

Step 14: Once you find the key, select **"Ciphertext"** in the Kasiski Examination tool to see the **decrypted plaintext.**

Step 15: **Add spaces between the words** in the plaintext, then **search it online to identify the song's title.**

Example:

Ciphertext:

```
everywhereimlookinnowimsurroundedbyyourembracebabyicanseeyourhaloyou
knowyouremysavingraceyoureeverythingineedandmoreitswrittenalloveryou
rfacebabyicanfeelyourhaloprayitwontfadeawayicanfeelyourhalohalohaloi
canseeyourhalohalohalo
```


Formatted plaintext:

everywhere im lookin now im surrounded by your embrace baby I can see your halo you know youre my savin grace youre everything I need and more its written all over your face baby I can feel your halo pray it wont fade away I can feel your halo halo halo i can see your halo halo halo

Song:

Genius
https://genius.com › Beyonce-halo-lyrics

Halo Lyrics - Beyoncé

Everywhere I'm lookin' now. I'm surrounded by your embrace · You know you're my savin' grace. You're everything I need and more · It's written all over your face

✓ **What is your song?**

_____

✓ **Who is the artist of the song?**

_____

End of the worksheet

Tip: If you're struggling to find your key, try a brute-force attack. 😉