CRYPTANALYSIS

FOR THIS UNIT...

01 CRYPTANALYSIS

02 BRUTE-FORCE ATTACK

03 DICTIONARY ATTACK

04 FREQUENCY ANALYSIS

FOR THIS UNIT...

05 KASISKI EXAMINATION

06 HILL CLIMBING

01

WHAT IS CRYPTANALYSIS?

Content Curated by Pollux M. Rey

CRYPTANALYSIS

The science of
unscrambling a message without knowledge of the key.

The Code Book, Singh

CRYPTOGRAPHER VS. CRYPTANALYST

CRYPTOGRAPHER

Develops new methods of secret writing

CRYPTANALYST

Finds weaknesses to break into secret messages

The Code Book, Singh

CRYPTANALYSIS

Requires advanced knowledge in **mathematics, statistics, and linguistics.**

The Code Book, Singh

02

BRUTE FORCE ATTACK

Content Curated by Pollux M. Rey

BRUTE-FORCE ATTACK

Tries every possible decryption key for a cipher.

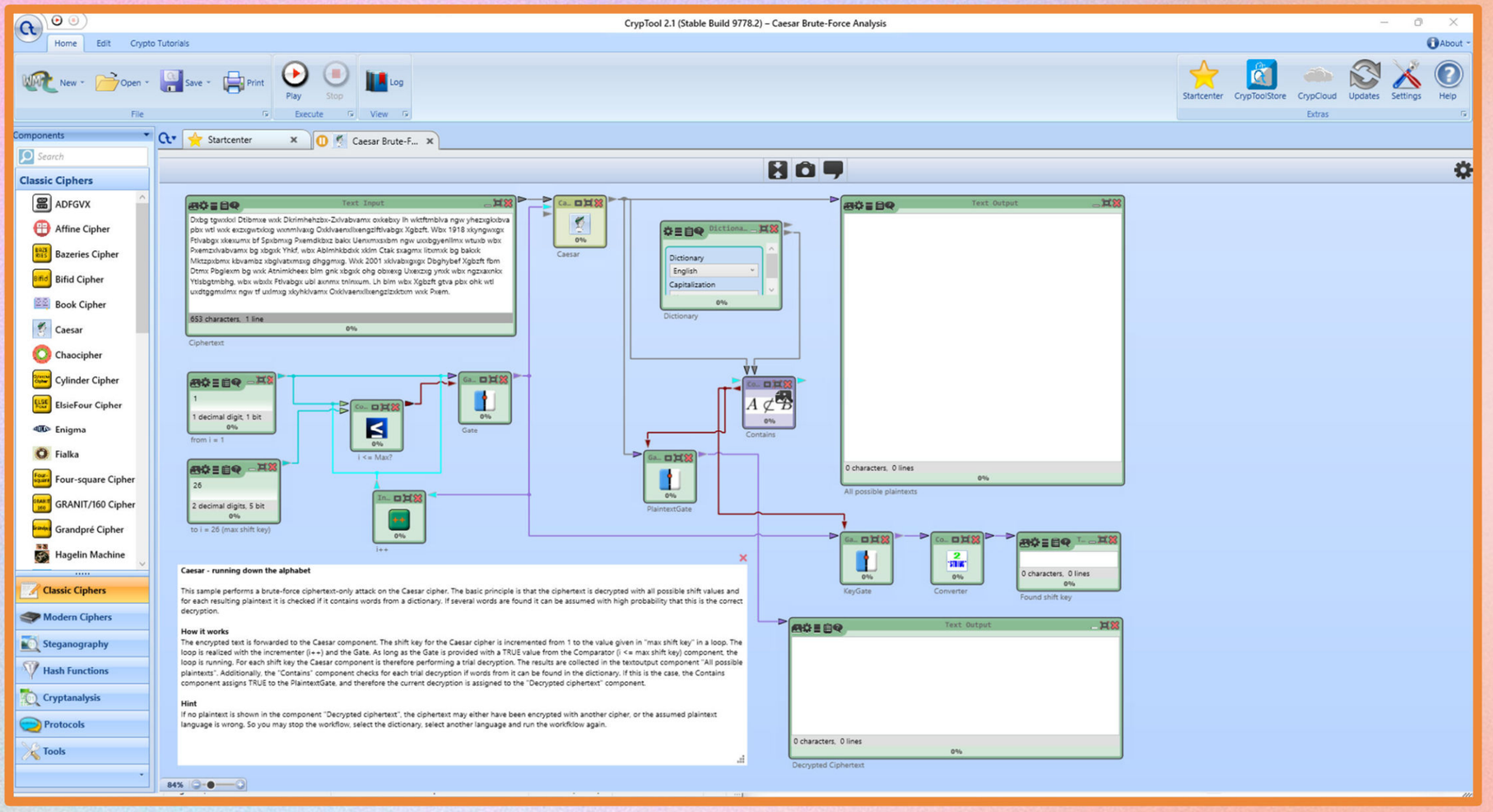
BRUTE-FORCE ATTACK

It is **effective against Caesar cipher.**

BRUTE-FORCE ATTACK

Any computer can **easily decrypt with all 26 possible keys**, and it takes a cryptanalyst only a few seconds to look through the decrypted messages to find the one in English.

BRUTE-FORCE ATTCK



BRUTE-FORCE ATTACK

However, when the **ciphertext alphabet is randomly arranged** instead of following alphabetical order, it is **effectively invulnerable to a brute-force attack** because it has an **enormous number of possible keys.**

Cracking Codes with Python, Sweigart

RANDOM CIPHERTEXT ALPHABET

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
V	J	Z	B	G	N	F	E	P	L	I	T	M	X	D	W	K	Q	U	C	R	Y	A	H	S	O

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
Z	Y	K	M	N	C	Q	V	R	P	L	B	A	J	T	I	D	H	X	E	G	F	W	O	U	S

⋮

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
U	I	F	L	J	B	X	Y	D	G	K	O	E	Q	T	H	S	R	A	V	C	P	N	Z	W	M

There are **403,291,461,126,605,635,584,000,000** different possible key orderings.

FREQUENCY ANALYSIS

Natural language is not random and this **does not hide the statistical properties of the natural language.**

Cracking Codes with Python, Sweigart

FREQUENCY ANALYSIS

We can also learn much about a ciphertext from the **frequency of its letters.**

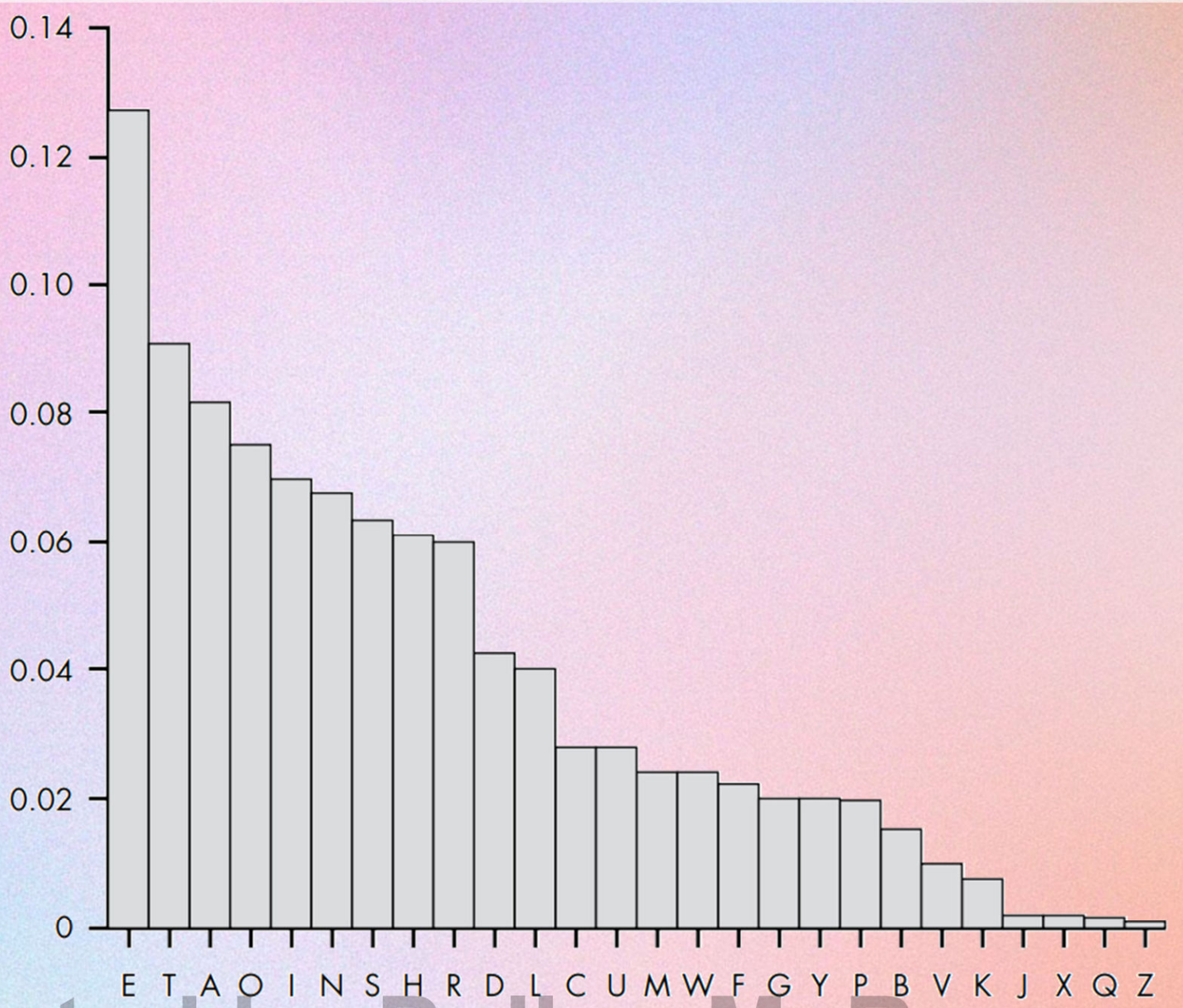
FREQUENCY ANALYSIS

We can also learn much about a ciphertext from the **frequency of its letters.**

FREQUENCY ANALYSIS

We will **use this difference in letter frequencies in the English language.**

COMMON ENGLISH LETTERS



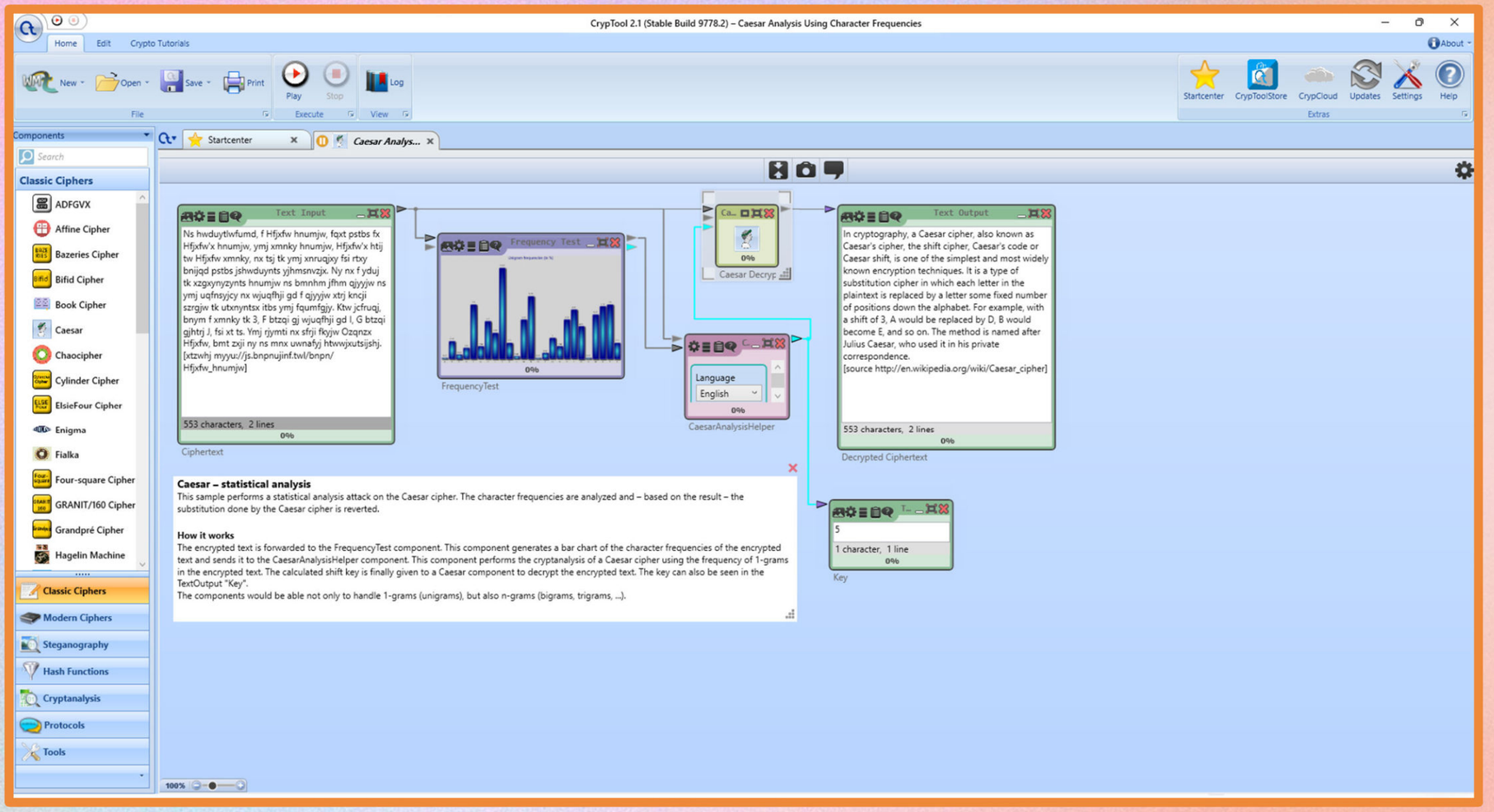
FREQUENCY ANALYSIS

The **letters that appear most often** are more likely to have been **encrypted from the most commonly found English letters**, such as E, T, or A.

FREQUENCY ANALYSIS

Similarly, the **letters that appear least often** in the ciphertext are **more likely to have been encrypted from to X, Q, and Z in plaintext.**

FREQUENCY ANALYSIS



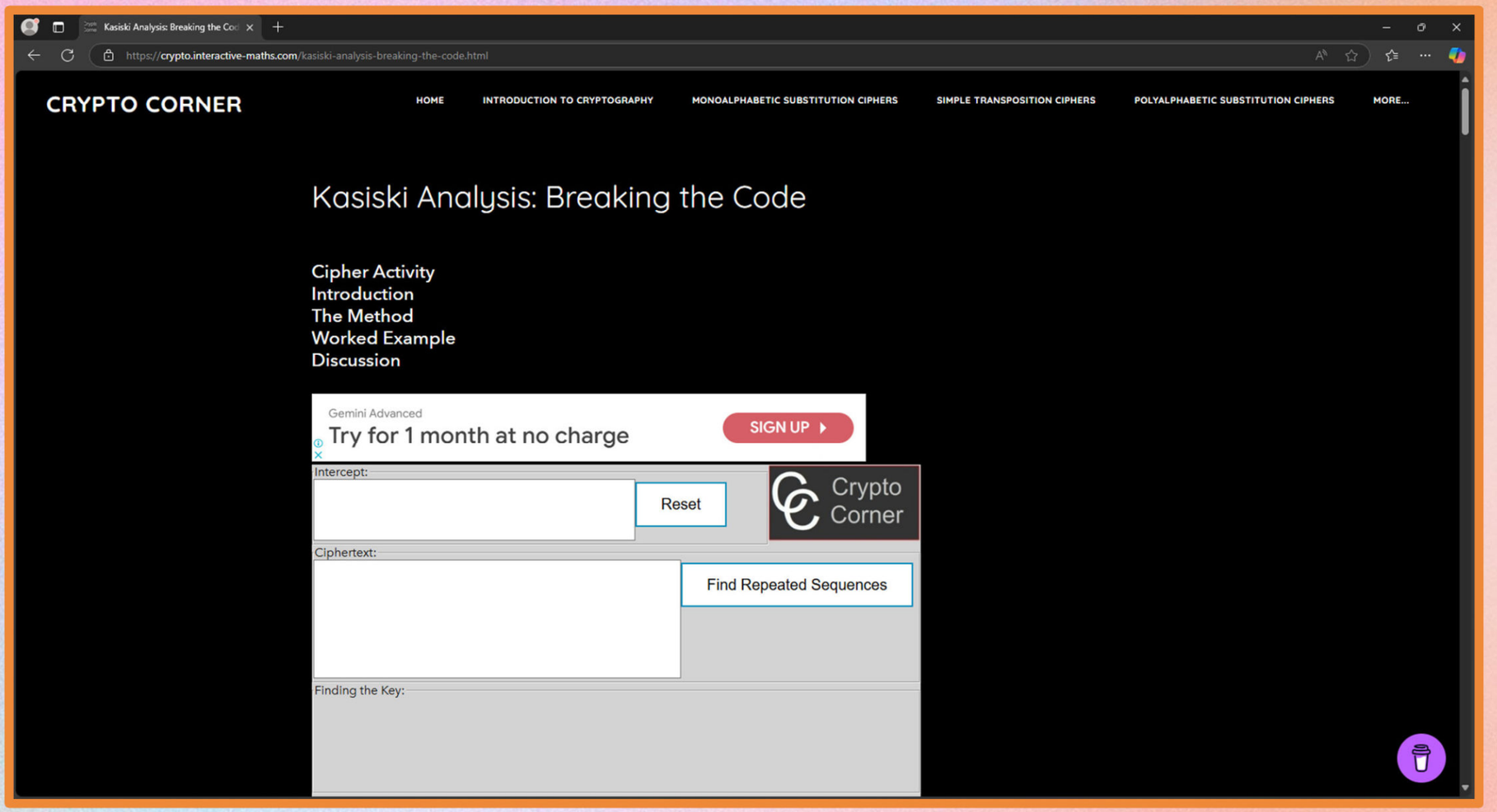
FREQUENCY ANALYSIS

You can also use it to **crack Vigenère cipher.**

FREQUENCY ANALYSIS

But first, you have to **guess the key length.**

KASISKI EXAMINATION



KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOFUISFYFBEXEINFIMAYSSDYYIJNPWTOKFRHWVWTZFXHLUYUMSGVD
URBWBIVXFAFMYFYXPIGBHWIFHHOJBEXAUNFIYLJWDKNHGAOVBHHGVINAULZFOFUQCVFBYNFTYGMMSVG
XCFZFOKQATUIFUFERQTEWZFOKMWOJYLNZBKSHOEBPNAYTFKNXLBVUAXCXUYYKYTFRHRCFUYCLUKTVGUF
QBESWYSSWLBYFEFZVUWTRLLNGIZGBMSZKBTNTSLNNMDPMYMIUBVMTLOBJHHFWTJNAUFIZMBZLIVHMBSU
WLBYFEUYFUFENBRVJVKOLLGTVUZUAOJNVUWTRLMBATZMFSSOJQXLFPKNAULJCIOYVDRYLUJMVMLVMUK
BTNAMFPXXJPDYFIJFYUWSGVIUMBWSTUXMSSNYKYDJMCGASOUXBYSMCMEUNFJNAUFUYUMWSFJUKQWS
VXXUVUFFBPWBCFYLWFDYGUKDRYLUJMFPXXEFZQXYHGFLACEBJBXQSTWIKNMORNXCJFAIBWWBKCMUKIV
QTMNBCCTHLJYIGIMSYCFVMURMAYOBJUFVAUZINMATCYPBANKBXLWJJNXUJTWIKBATCIOYBPPZHLZJJZHL
LVEYAIFPLLYIJIZMOUDPLLTHVEVUMBXPIBBMSNSCMCGONBHCKIVLXMGCRMXNZBKQHODESYTVGOUGTHAG
RHRMHFREYIJIZGAUNFZIYZWOUYWQZPZMAYJFJIKOVFKBTNOPLFWHGUSYTLGNRHBZSOPMIYSLWIKBANYUO
YAPWZXHVFUQAIATYYKYKPMCEYLIRNPCDMEIMFGWVBBMUPLHMLQJWUGSKQVUDZGSYCFBSWVCHZXFEXX
XAQROLYXPIUKYHMPNAYFOFHXBSWVCHZXFEXXXAIRPXXGOVHHGGSVNHWSFJUKNZBESHOKIRFEXGUFVKO
LVJNAYIVVMMCGOFZACKEVUMBATVHKIDMVXBHLIVWTJAUFFACKHCIKSFPKYQNWOLUMYVXYYKYAOYYPUK
XFLMBQOFLACKPWZXHUFJYGZGSTYWZGSNBBWZIVMNZXFIYWXWBKBAYJFTIFYKIZMUIVZDINLFFUVRGSSBU
GNGOPQAILIFOZBZFYUWHGIRHWCFIZMWYSUYMAUDMIYVYAWVNAYTFEYYCLPWBBMVZZHZUHMRWXCFUYY
VIENFHPYSMKBTMOIZWAIXZFOLBSMCHHNOJKBMBATZXXJSSKNAULBJCLFWXDSUYKUCIOYJGFLMBWHFIWIX
SFGXCZBMYMBWTRGXXSHXYKZGSDSLYDGNBXHAUJBTFDQCYTMWNPWHOFUISMIFFVXFSVFRNA

KASISKI EXAMINATION

Repeated Sequences	Distance	Factors
ZFOK	18	1, 2, 3, 6, 9, 18
WLBY	72	1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72
FUFE	156	1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156
VUWT	96	1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96
NAUL	240	1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120, 240

KASISKI EXAMINATION

Repeated Sequences	Distance	Factors
ZFOK	18	**1**, **2**, **3**, **6**, 9, 18
WLBY	72	**1**, **2**, **3**, 4, **6**, 8, 9, 12, 18, 24, 36, 72
FUFE	156	**1**, **2**, **3**, 4, **6**, 12, 13, 26, 39, 52, 78, 156
VUWT	96	**1**, **2**, **3**, 4, **6**, 8, 12, 16, 24, 32, 48, 96
NAUL	240	**1**, **2**, **3**, 4, 5, **6**, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120, 240

The possible key lengths are **1, 2, 3, and 6.**

KASISKI EXAMINATION

Now that we have possible lengths of the Vigenère key, we can use this information to decrypt the message one subkey at a time.

KASISKI EXAMINATION

If the **key length is 6, every sixth letter in the ciphertext is encrypted** using the corresponding subkey, starting from the first letter for the first subkey, the second letter for the second subkey, and so on.

KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

Ciphertext:

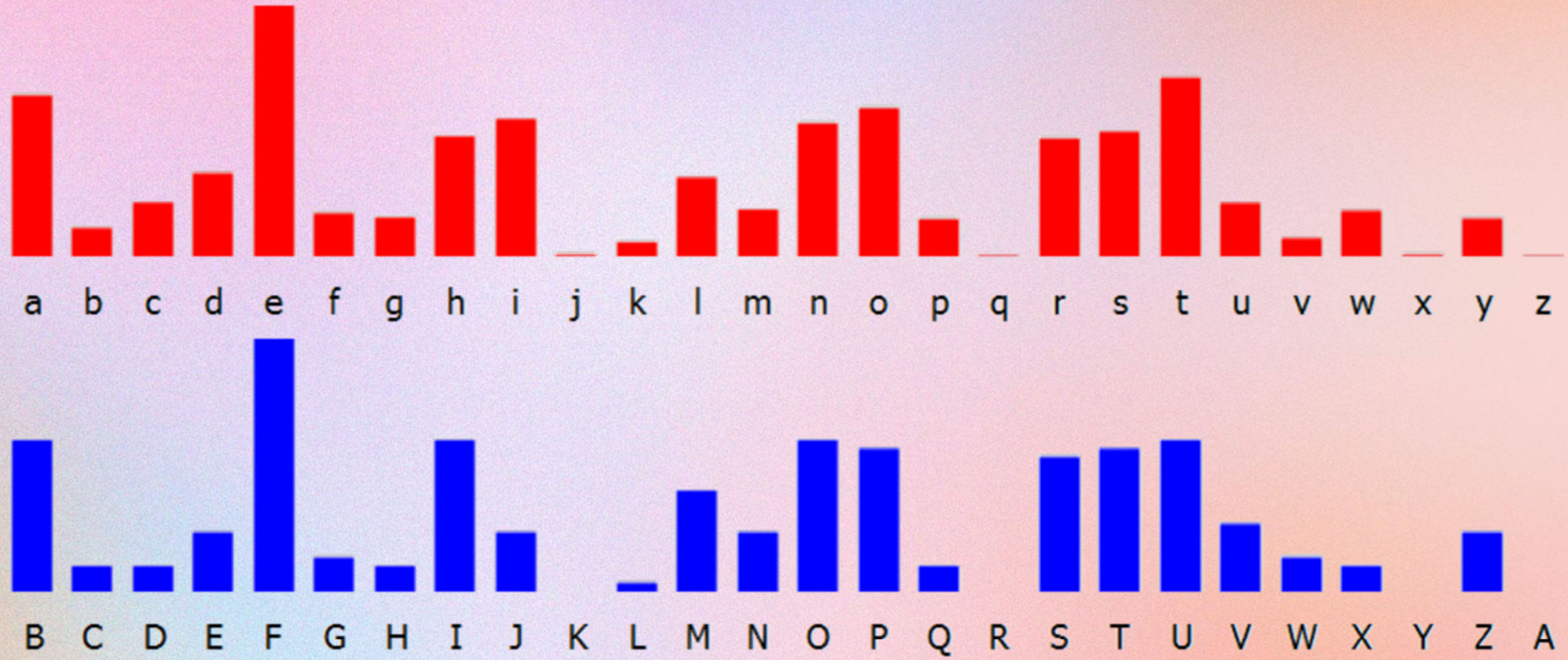
CVJTNAFENMCDMKBXFSTKLHGSOJWHOF...

KASISKI EXAMINATION

After determining the possible key length, **Frequency Analysis will be applied to each group to identify the most likely subkey.**

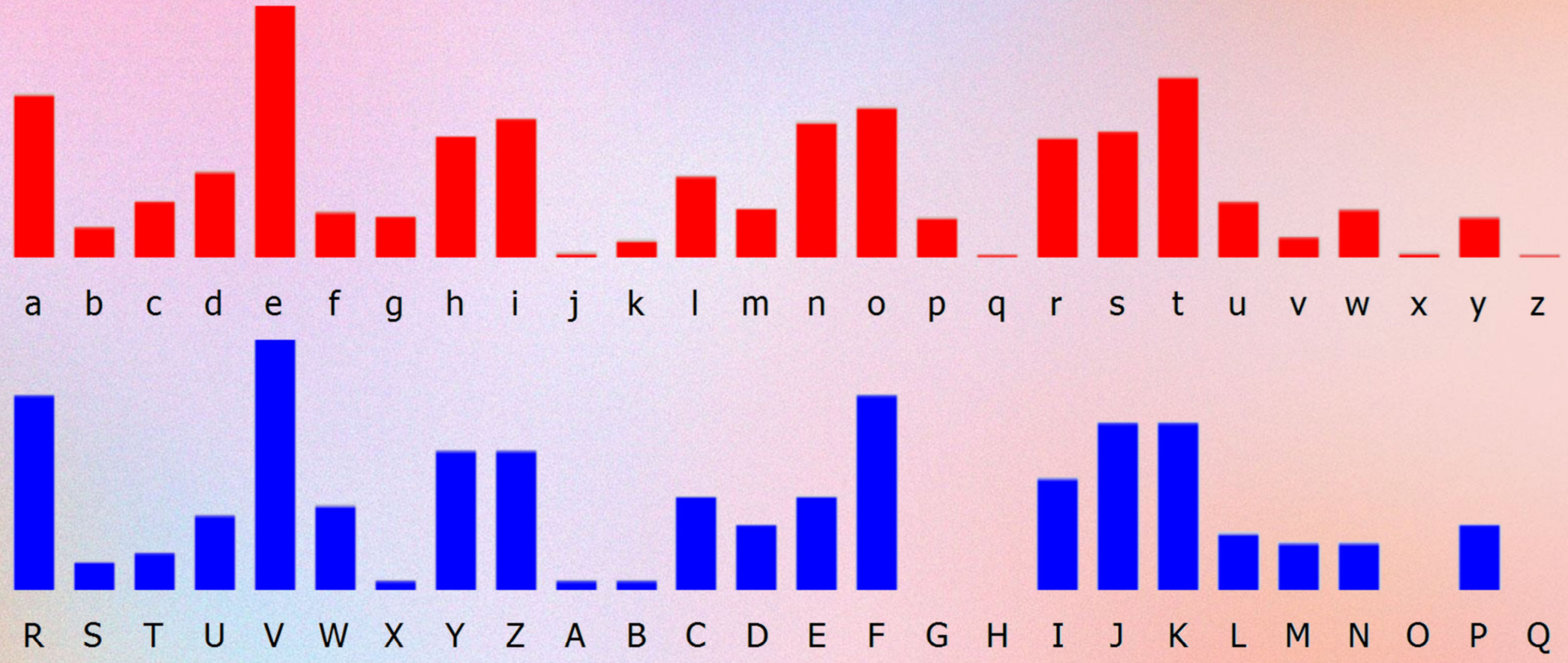
FREQUENCY ANALYSIS

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



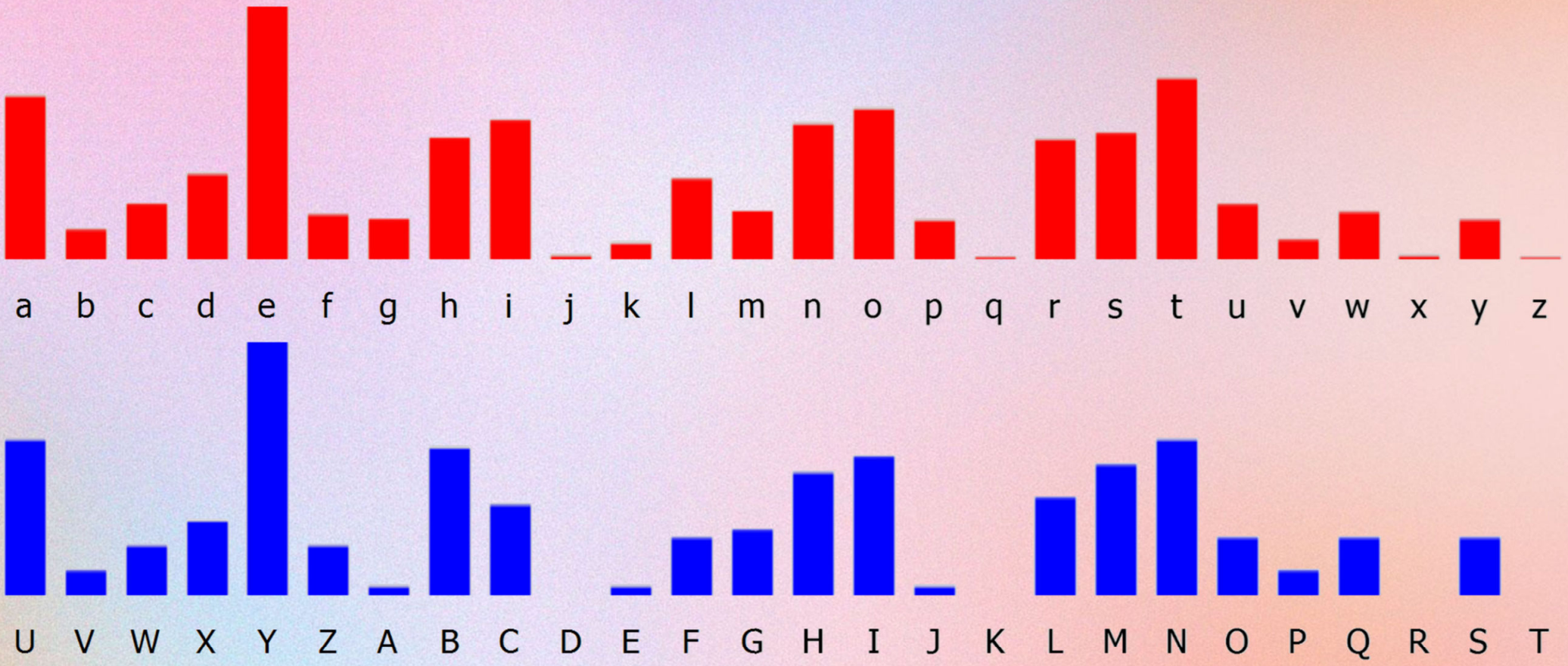
FREQUENCY ANALYSIS

The **second subkey was shifted by 17**, which corresponds to the letter **R.**



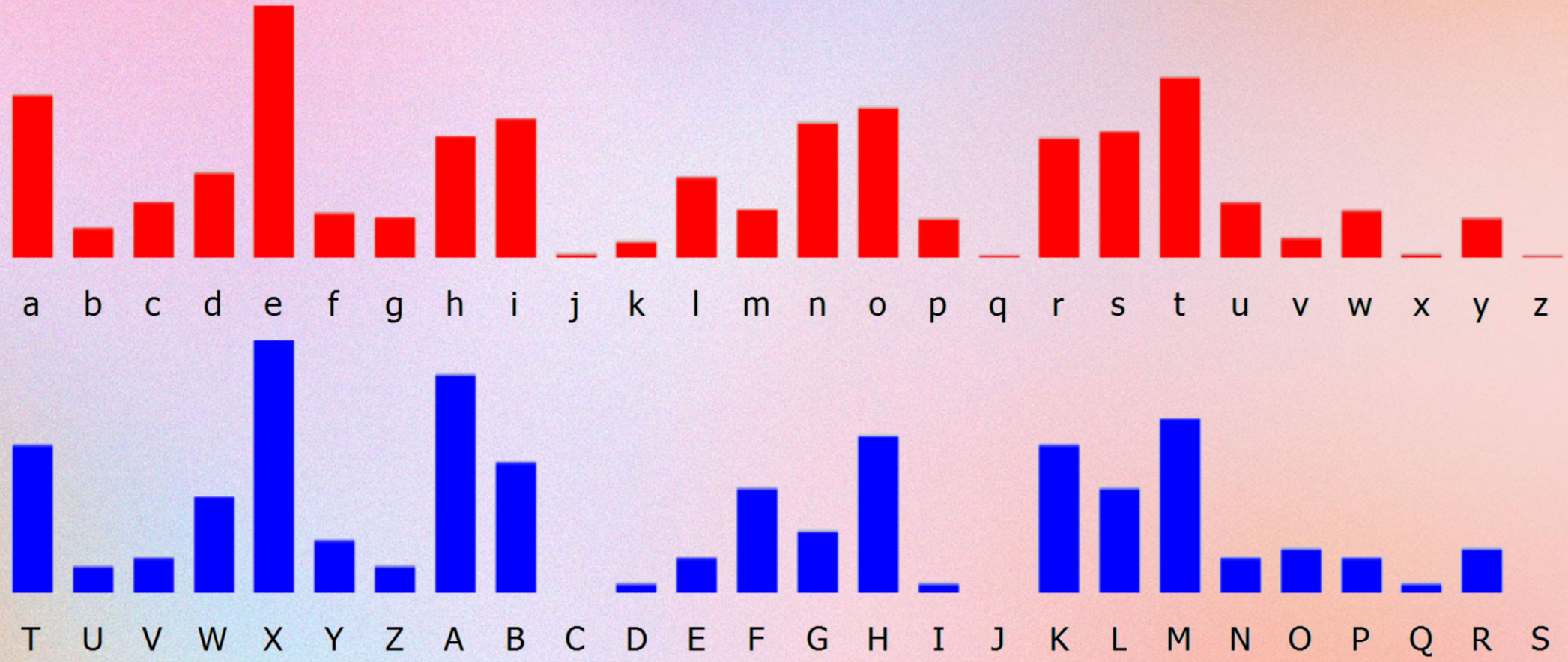
FREQUENCY ANALYSIS

The **third subkey was shifted by 20**, which corresponds to the letter **U**.



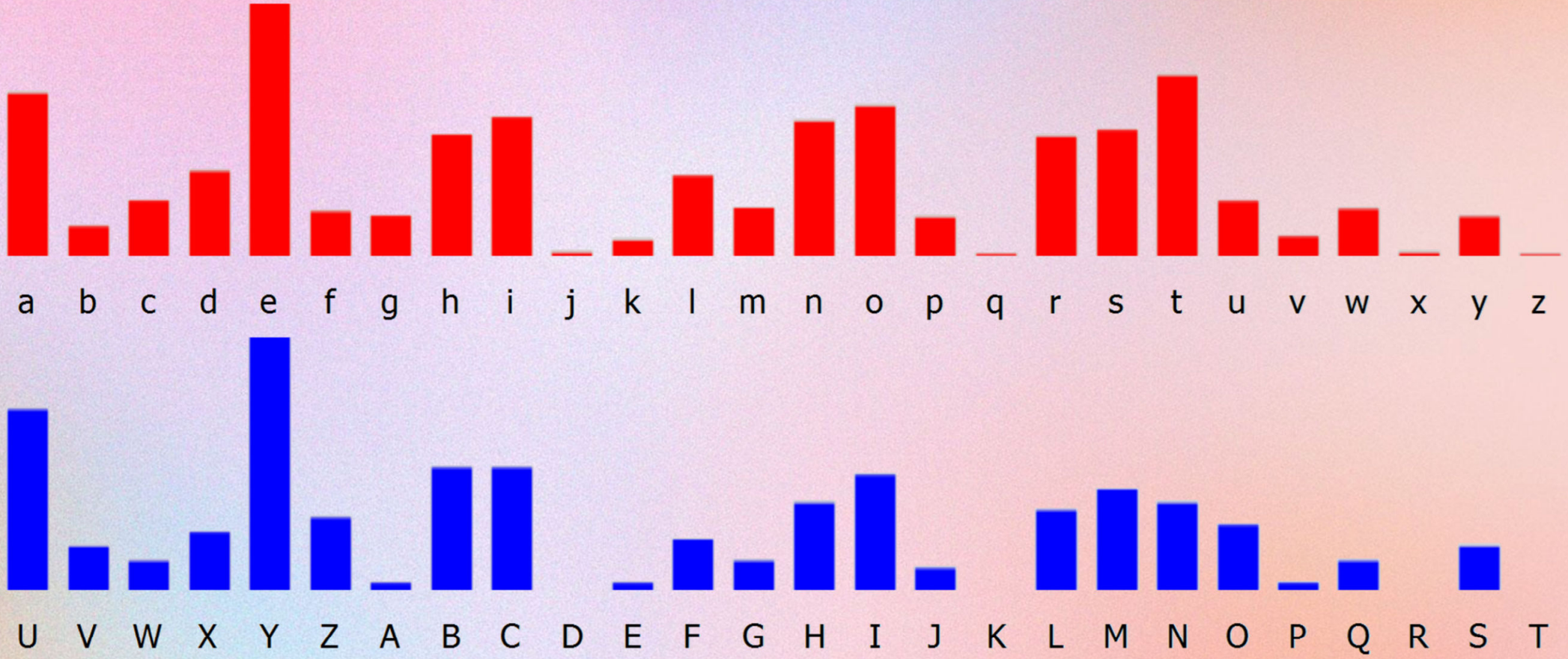
FREQUENCY ANALYSIS

The **fourth subkey was shifted by 19**, which corresponds to the letter **T**.



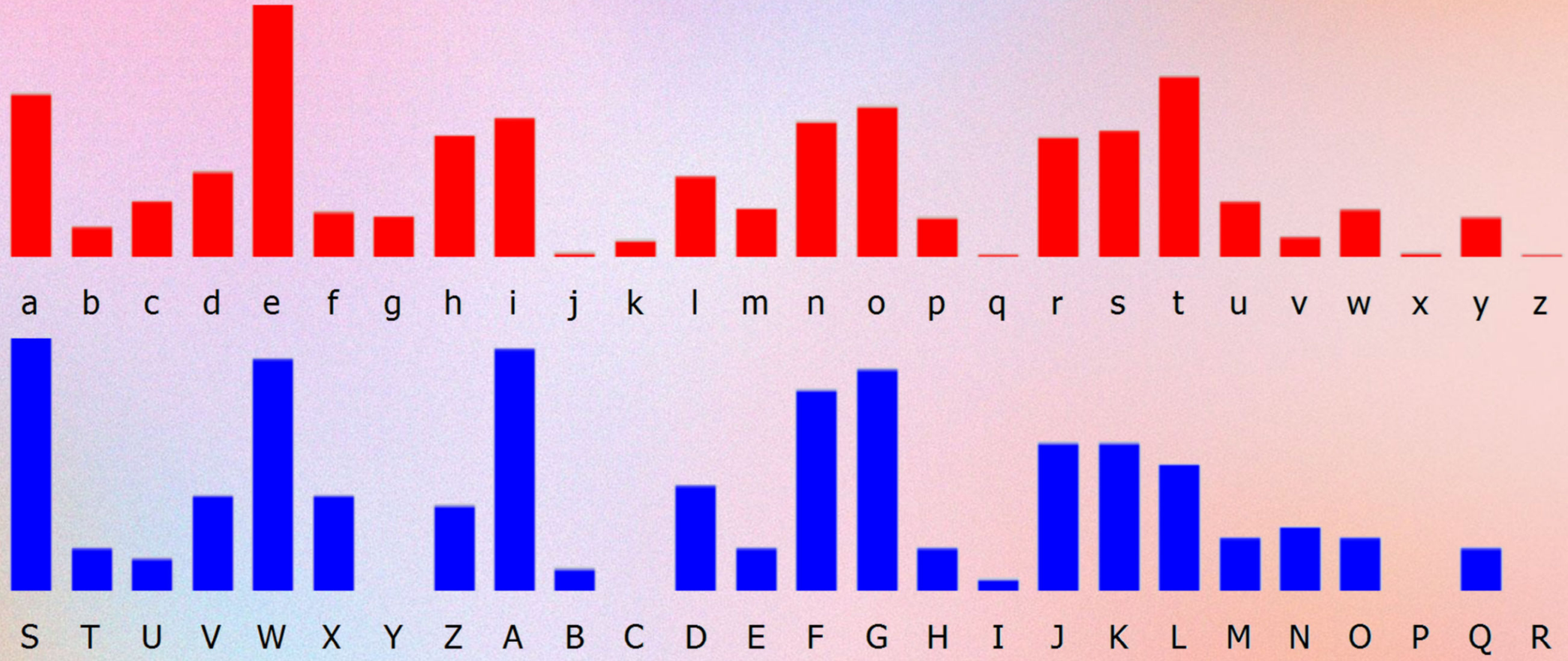
FREQUENCY ANALYSIS

The **fifth subkey was shifted by 20**, which corresponds to the letter **U**.



FREQUENCY ANALYSIS

The **fifth subkey was shifted by 18**, which corresponds to the letter **S**.



FREQUENCY ANALYSIS

Key:

BRUTUS

FREQUENCY ANALYSIS

Ciphertext:

CVJTNAFENMCDMKBXFSTKLHGSOJWHOFUISFYFBEXEINFIMAYSSDYYIJNPWTOKFRHWVWTZFXHLUYUMSGVD
URBWBIVXFAFMYFYXPIGBHWIFHHOJBEXAUNFIYLJWDKNHGAOVBHHGVINAULZFOFUQCVFBYNFTYGMMSVG
XCFZFOKQATUIFUFERQTEWZFOKMWOJYLNZBKSHOEBPNAYTFKNXLBVUAXCXUYYKYTFRHRCFUYCLUKTVGUF
QBESWYSSWLBYFEFZVUWTRLLNGIZGBMSZKBTNTSLNNMDPMYMIUBVMTLOBJHHFWTJNAUFIZMBZLIVHMBSU
WLBYFEUYFUFENBRVJVKOLLGTVUZUAOJNVUWTRLMBATZMFSSOJQXLFPKNAULJCIOYVDRYLUJMVMLVMUK
BTNAMFPXXJPDYFIJFYUWSGVIUMBWSTUXMSSNYKYDJMCGASOUXBYSMCMEUNFJNAUFUYUMWSFJUKQWS
VXXUVUFFBPWBCFYLWFDYGUKDRYLUJMFPXXEFZQXYHGFLACEBJBXQSTWIKNMORNXCJFAIBWWBKCMUKIV
QTMNBCCTHLJYIGIMSYCFVMURMAYOBJUFVAUZINMATCYPBANKBXLWJJNXUJTWIKBATCIOYBPPZHLZJJZHL
LVEYAIFPLLYIJIZMOUDPLLTHVEVUMBXPIBBMSNSCMCGONBHCKIVLXMGCRMXNZBKQHODESYTVGOUGTHAG
RHRMHFREYIJIZGAUNFZIYZWOUYWQZPZMAYJFJIKOVFKBTNOPLFWHGUSYTLGNRHBZSOPMIYSLWIKBANYUO
YAPWZXHVFUQAIATYYKYKPMCEYLIRNPCDMEIMFGWVBBMUPLHMLQJWUGSKQVUDZGSYCFBSWVCHZXFEXX
XAQROLYXPIUKYHMPNAYFOFHXBSWVCHZXFEXXXAIRPXXGOVHHGGSVNHWSFJUKNZBESHOKIRFEXGUFVKO
LVJNAYIVVMMCGOFZACKEVUMBATVHKIDMVXBHLIVWTJAUFFACKHCIKSFPKYQNWOLUMYVXYYKYAOYYPUK
XFLMBQOFLACKPWZXHUFJYGZGSTYWZGSNBBWZIVMNZXFIYWXWBKBAYJFTIFYKIZMUIVZDINLFFUVRGSSBU
GNGOPQAILIFOZBZFYUWHGIRHWCFIZMWYSUYMAUDMIYVYAWVNAYTFEYYCLPWBBMVZZHZUHMRWXCFUYY
VIENFHPYSMKBTMOIZWAIXZFOLBSMCHHNOJKBMBATZXXJSSKNAULBJCLFWXDSUYKUCIOYJGFLMBWHFIWIX
SFGXCZBMYMBWTRGXXSHXYKZGSDSLYDGNBXHAUJBTFDQCYTMWNPWHOFUISMIFFVXFSVFRNA

FREQUENCY ANALYSIS

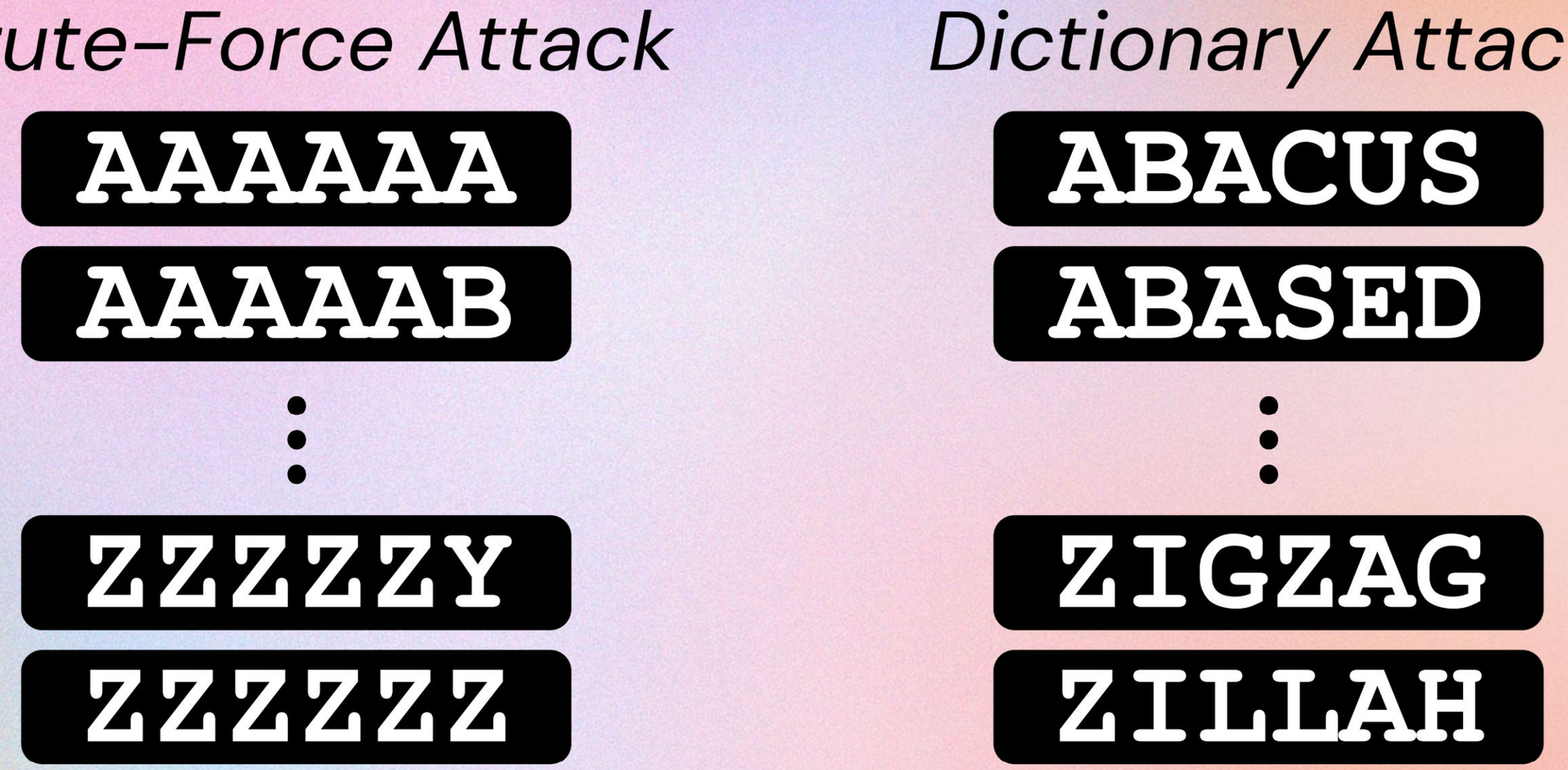
Plaintext:

BEPATIENTTILLTHELASTROMANSCOUNTRYMENANDLOVERSHEARMEFORMYCAUSEANDBESILENTTHATYOUM
AYHEARBELIEVEMEFORMINEHONOURANDHAVERESPECTTOMINEHONOURTHATYOUMAYBELIEVECENSUREMEI
NYOURWISDOMANDAWAKEYOURSENSESTHATYOUMAYTHEBETTERJUDGEIFTHEREBEANYINTHISASSEMBLYAN
YDEARFRIENDOFCAESARSTOHIMISAYTHATBRUTUSLOVETOCAESARWASNOLESSTHANHISIFTHENTHATFRIEND
DEMANDWHYBRUTUSROSEAGAINSTCAESARTHISISMYANSWERNOTTHATILOVEDCAESARLESSBUTTHATILOVE
DROMEMOREHADYOURATHERCAESARWERELIVINGANDDIEALLSLAVESTHANTHATCAESARWEREDEADTOLIVE
ALLFREEMENASCAESARLOVEDMEIWEEPFORHIMASHEWASFORTUNATEIREJOICEATITASHEWASVALIANTIHON
OURHIMBUTASHEWASAMBITIOUSISLEWHIMTHEREISTEARSFORHISLOVEJOYFORHISFORTUNEHONOURFORHIS
VALOURANDDEATHFORHISAMBITIONWHOISHERESOBASETHATWOULDBEABONDMANIFANYSPEAKFORHIMHA
VEIOFFENDEDWHOISHERESORUDETHATWOULDNOTBEAROMANIFANYSPEAKFORHIMHAVEIOFFENDEDWHOIS
HERESOVILETHATWILLNOTLOVEHISCOUNTRYIFANYSPEAKFORHIMHAVEIOFFENDEDIPAUSEFORAREPLYTHENN
ONEHAVEIOFFENDEDIHAVEDONENOMORETOCAESARTHANYOUSHALLDOTOBRUTUSTHEQUESTIONOFHISDEA
THISENROLLEDINTHECAPITOLHISGLORYNOTEXTENUATEDWHEREINHEWASWORTHYNORHISOFFENCESENFOR
CEDFORWHICHHESUFFEREDDEATHHERECOMESHISBODYMOURNEDBYMARKANTONYWHOTHOUGHHEHADNO
HANDINHISDEATHSHALLRECEIVETHEBENEFITOFHISDYINGAPLACEINTHECOMMONWEALTHASWHICHOFYOUS
HALLNOTWITHTHISIDEPARTTHATASISLEWMYBESTLOVERFORTHEGOODOFROMEIHAVETHESAMEDAGGERFOR
MYSELFWHENITSHALLPLEASEMYCOUNTRYTONEEDMYDEATH

DICTIONARY ATTACK

Besides Kasiski Examination and Frequency Analysis, you can use a **dictionary attack**, a type of brute-force attack, to find the Vigenère key.

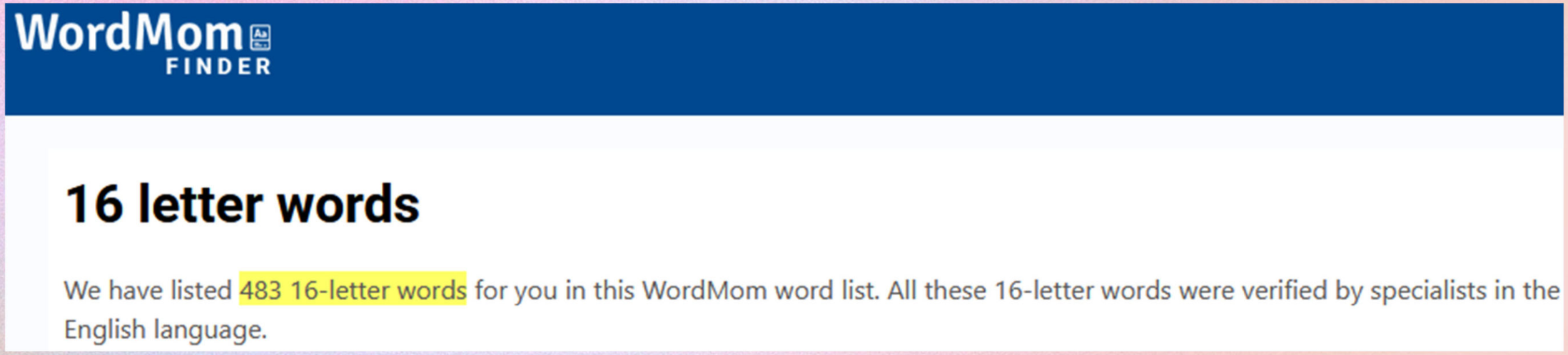
BRUTE-FORCE VS. DICTIONARY ATTACK



BRUTE-FORCE ATTACK

Key length	Equation	Possible keys
1	26	= 26
2	26 × 26	= 676
3	676 × 26	= 17,576
4	17,576 × 26	= 456,976
5	456,976 × 26	= 11,881,376
6	11,881,376 × 26	= 308,915,776
7	308,915,776 × 26	= 8,031,810,176
8	8,031,810,176 × 26	= 208,827,064,576
9	208,827,064,576 × 26	= 5,429,503,678,976
10	5,429,503,678,976 × 26	= 141,167,095,653,376
11	141,167,095,653,376 × 26	= 3,670,344,486,987,776
12	3,670,344,486,987,776 × 26	= 95,428,956,661,682,176
13	95,428,956,661,682,176 × 26	= 2,481,152,873,203,736,576
14	2,481,152,873,203,736,576 × 26	= 64,509,974,703,297,150,976

DICTIONARY ATTACK



PLAYFAIR CIPHER

*"**Manually breaking** a Playfair cryptogram is a difficult task."*

Content Curated by Pollux M. Rey

Codebreaking: A practical guide, Dunin and Schmeh

PLAYFAIR CIPHER

It requires **reconstructing the 5×5 key square** by **identifying digraph patterns** in the ciphertext.

Codebreaking: A practical guide, Dunin and Schmeh

HILL CLIMBING

Takes a random key and checks whether the plaintext obtained with it **looks like real language.**

Codebreaking: A practical guide, Dunin and Schmeh

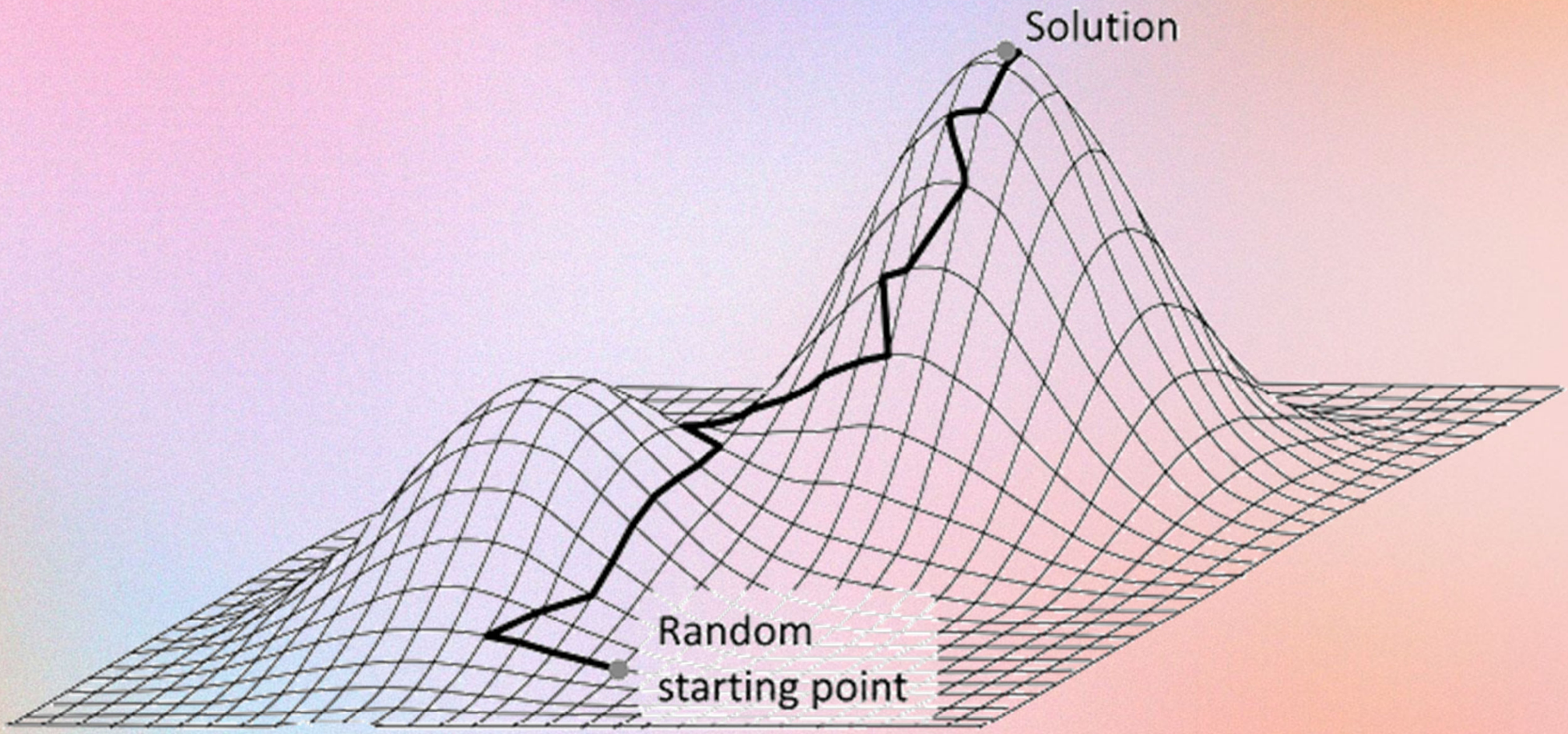
HILL CLIMBING

By making small changes to the key, it tries to improve the result **until no better one can be found.**

The last candidate often is the correct one.

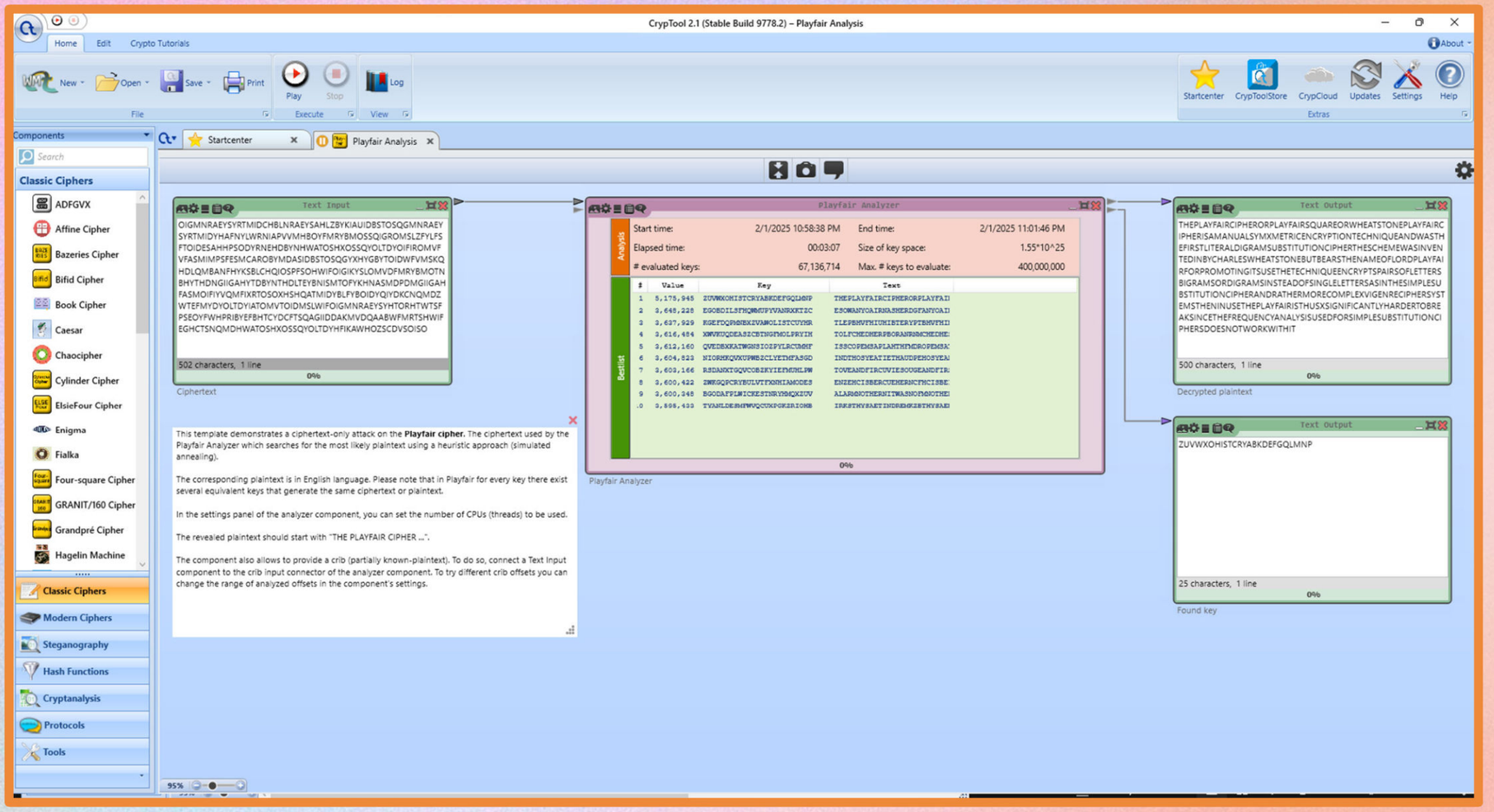
Codebreaking: A practical guide, Dunin and Schmeh

HILL CLIMBING



Codebreaking: A practical guide, Dunin and Schmeh

HILL CLIMBING



RAIL FENCE CIPHER

"The essential technique is ***anagramming – rearranging the ciphertext letters to 'make sense.'"***

Content Curated by Pollux M. Rey

Kentucky State University

THANK YOU!

Content Curated by Pollux M. Rey