Cryptography: Vigenère and Kasiski

Alex Corner

Sheffield Hallam University

The Story So Far

- Classical ciphers generally used one of two methods:

The Story So Far

- Classical ciphers generally used one of two methods:
  - **Transposition:** Rearranging the characters of the message.

The Story So Far

- Classical ciphers generally used one of two methods:
  - **Transposition:** Rearranging the characters of the message.
  - **Substitution:** Disguise each letter as another.

The Story So Far

- Classical ciphers generally used one of two methods:
  - **Transposition:** Rearranging the characters of the message.
  - **Substitution:** Disguise each letter as another.
- Simple ciphers of either type were quite easily broken: substitution ciphers suffered from attacks using **frequency analysis**.

The Story So Far

- Classical ciphers generally used one of two methods:
  - **Transposition:** Rearranging the characters of the message.
  - **Substitution:** Disguise each letter as another.
- Simple ciphers of either type were quite easily broken: substitution ciphers suffered from attacks using **frequency analysis**.
- The Vigenère cipher was developed and was thought to tackle these problems.

Vigenère Cipher

- Shortcomings of the general substitution cipher were addressed in the 15th century.

Vigenère Cipher

- Shortcomings of the general substitution cipher were addressed in the 15th century.
- The solution: don't rely on just one substitution alphabet.

Vigenère Cipher

- Shortcomings of the general substitution cipher were addressed in the 15th century.
- The solution: don't rely on just one substitution alphabet.
- Instead of a *mono*alphabetic cipher, a **polyalphabetic** cipher was designed.

Vigenère Cipher

- Shortcomings of the general substitution cipher were addressed in the 15th century.
- The solution: don't rely on just one substitution alphabet.
- Instead of a *mono*alphabetic cipher, a **polyalphabetic** cipher was designed.
- The use of polyalphabetic ciphers is thought to have originated with Leon Battista Alberti in 1467.

Vigenère Cipher

- Attributed to Blaise de Vigenère, it was known as 'le chiffre indéchiffrable': the unbreakable cipher. As it turns out, de Vigenère's original cipher was actually more secure than that which came to bear his name.
- Used for many centuries, this was the state of the art, and truly thought to be unbreakable.

Vigenère Cipher

- The cipher depends on a keyword and the use of twenty six shifted alphabets.

Vigenère Cipher

- The cipher depends on a keyword and the use of twenty six shifted alphabets.
- The alphabets form a square: the Vigenère square, or *tabula recta*.

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

Vigenère Cipher

- Plaintext: `invade at dawn on friday`. Keyword: `CODES`.

Vigenère Cipher

- Plaintext: `invade at dawn on friday`. Keyword: `CODES`.
- The keyword is written repeatedly along the message. We look up the row of the key and match it to the column of the plaintext: row `C` and column `i` gives ciphertext `K`.

key	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S
plain	i	n	v	a	d	e	a	t	d	a	w	n	o	n	f	r	i	d	a	y
cipher	K	B	Y	E	V	G	O	W	H	S	Y	B	R	R	X	T	W	G	E	Q

Vigenère Cipher

- Plaintext: `invade at dawn on friday`. Keyword: `CODES`.
- The keyword is written repeatedly along the message. We look up the row of the key and match it to the column of the plaintext: row `C` and column `i` gives ciphertext `K`.

key	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S
plain	i	n	v	a	d	e	a	t	d	a	w	n	o	n	f	r	i	d	a	y
cipher	K	B	Y	E	V	G	O	W	H	S	Y	B	R	R	X	T	W	G	E	Q

- Can also be thought of in terms of modular arithmetic:

keyword	2	14	3	4	18	2	14	3	4	18	2	14	3
plaintext	8	13	21	0	3	4	0	19	3	0	22	13	14
ciphertext	10	1	24	4	21	6	14	22	7	18	24	1	17

Vigenère Cipher

- Plaintext: `invade at dawn on friday`. Keyword: `CODES`.
- The keyword is written repeatedly along the message. We look up the row of the key and match it to the column of the plaintext: row `C` and column `i` gives ciphertext `K`.

key	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S	C	O	D	E	S
plain	i	n	v	a	d	e	a	t	d	a	w	n	o	n	f	r	i	d	a	y
cipher	K	B	Y	E	V	G	O	W	H	S	Y	B	R	R	X	T	W	G	E	Q

- Can also be thought of in terms of modular arithmetic:

keyword	2	14	3	4	18	2	14	3	4	18	2	14	3
plaintext	8	13	21	0	3	4	0	19	3	0	22	13	14
ciphertext	10	1	24	4	21	6	14	22	7	18	24	1	17

- Encryption is achieved by performing the addition

$$c_i = m_i + k_i \mod 26,$$

where m_i is the ith letter of the message and k_i is the ith letter of the keyword repeated over and over again.

Vigenère Cipher

- The plaintext `invade at dawn on friday` has become the ciphertext

  KBYEVGOWHSYBRRXTWGEQ.

Vigenère Cipher

- The plaintext `invade at dawn on friday` has become the ciphertext

  KBYEVGOWHSYBRRXTWGEQ.

- This is much more secure than a monoalphabetic substitution: the three `d` characters in the plaintext are encrypted differently each time as `V`, `H`, and `G`.

Vigenère Cipher

- The plaintext `invade at dawn on friday` has become the ciphertext

  KBYEVGOWHSYBRRXTWGEQ.

- This is much more secure than a monoalphabetic substitution: the three `d` characters in the plaintext are encrypted differently each time as `V`, `H`, and `G`.
- Our simple frequency analysis will not work any more and this type of cipher was thought unbreakable right up until the end of World War 1 (1914-1918).

Vigenère Cipher

- The plaintext `invade at dawn on friday` has become the ciphertext

  KBYEVGOWHSYBRRXTWGEQ.

- This is much more secure than a monoalphabetic substitution: the three `d` characters in the plaintext are encrypted differently each time as `V`, `H`, and `G`.
- Our simple frequency analysis will not work any more and this type of cipher was thought unbreakable right up until the end of World War 1 (1914-1918).
- A few people were involved in the cracking of this cipher, including quite a famous name in computing history.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:
  - If the **key length** is discovered, then we can apply frequency analysis, given a long enough message.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:
  - If the **key length** is discovered, then we can apply frequency analysis, given a long enough message.
  - Suppose the key length is $k = 5$.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:
  - If the **key length** is discovered, then we can apply frequency analysis, given a long enough message.
  - Suppose the key length is $k = 5$.
  - We can apply frequency analysis on groups of letters which are separated by five letters: the key length.

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:
  - If the **key length** is discovered, then we can apply frequency analysis, given a long enough message.
  - Suppose the key length is $k = 5$.
  - We can apply frequency analysis on groups of letters which are separated by five letters: the key length.
  - ANYVGYSTYNRPLWH...

Vigenère Cipher

- On the face of it, this new method is resistant to attacks using frequency analysis.
- There is a very large keyspace (number of keys), which depends on the length of the key used.
  - For a key of length 5, there are 11881376 different possibilities:

$$26^5 = 11881376.$$

- But it turns out we can still use frequency analysis, we just have to be a bit more clever in its use:
  - If the **key length** is discovered, then we can apply frequency analysis, given a long enough message.
  - Suppose the key length is $k = 5$.
  - We can apply frequency analysis on groups of letters which are separated by five letters: the key length.
  - ANYVGYSTYNRPLWH...
  - These letters must have used the same row of the Vigenère square.

Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

- Assume we know the key length: $k = 6$. We'll look into how to figure this out later.

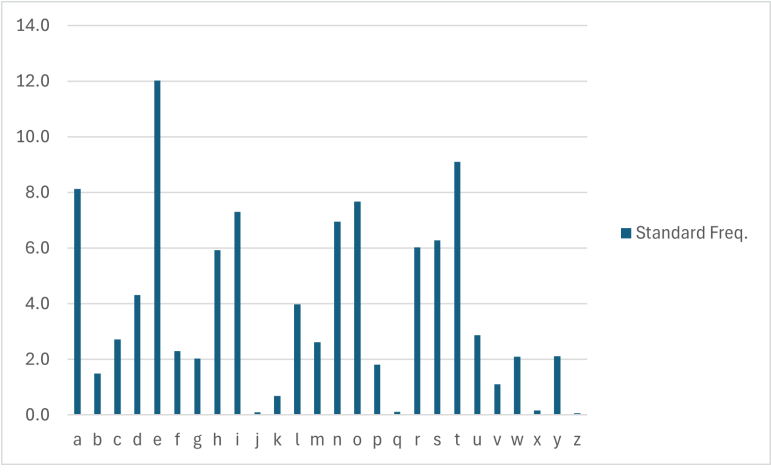
Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

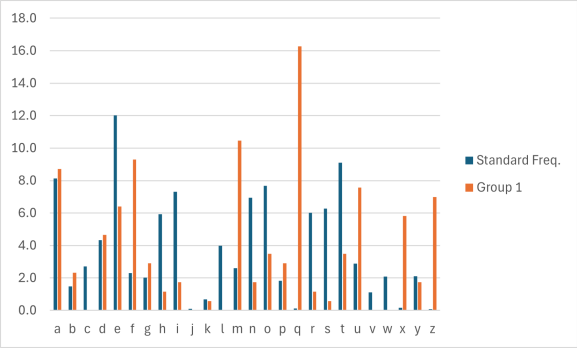
Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

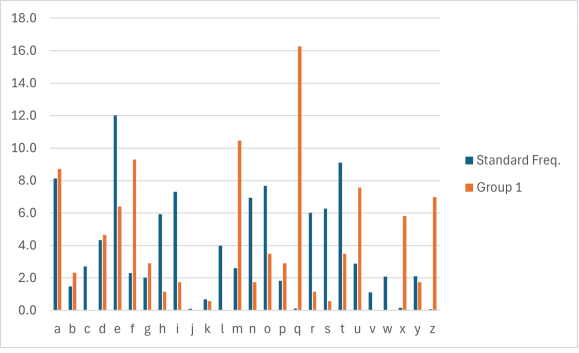
Patterns in the Standard Frequencies



Letter Group 1

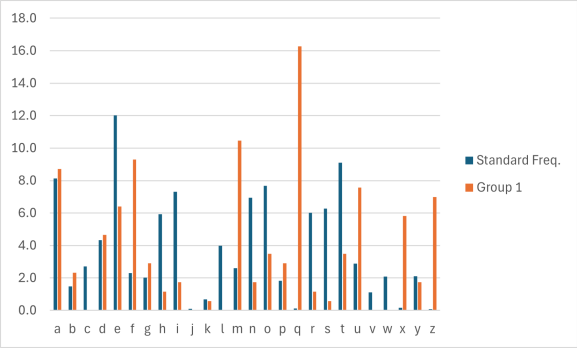


Letter Group 1



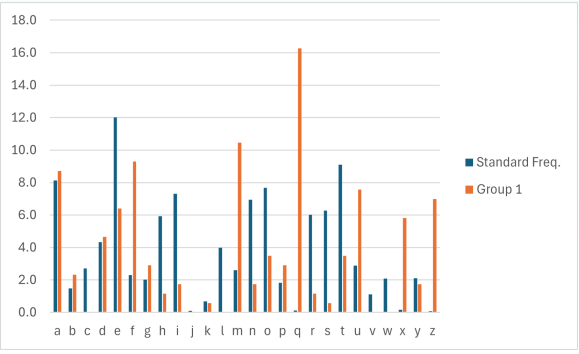
- Each group has been shifted by the same value: a Caesar cipher.

Letter Group 1



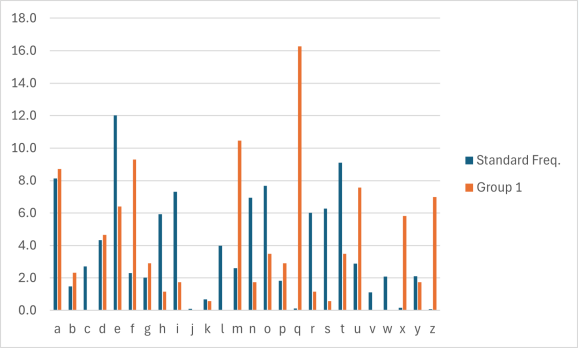
- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.

Letter Group 1



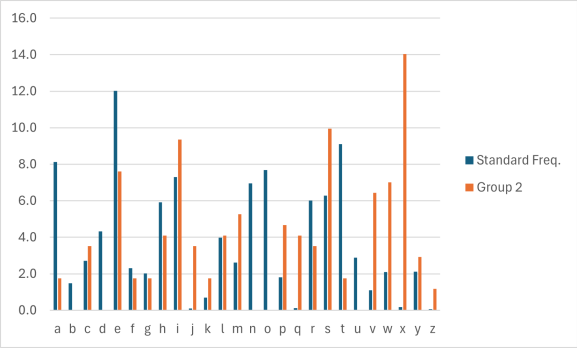
- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.
- There is a gap of 4 letters from a to e, with e having the higher frequency.

Letter Group 1

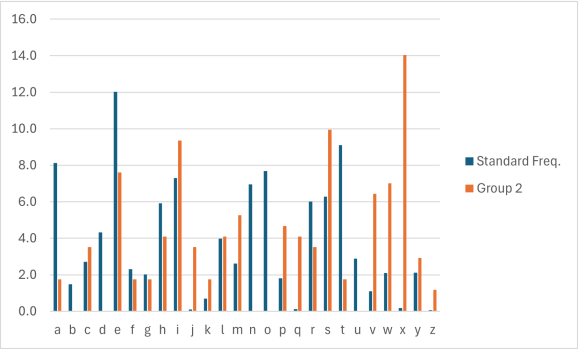


- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.
- There is a gap of 4 letters from a to e, with e having the higher frequency.
- We can find this same gap, or other patterns, and deduce that the likely shift is a to `m`: shift value 12.

Letter Group 2

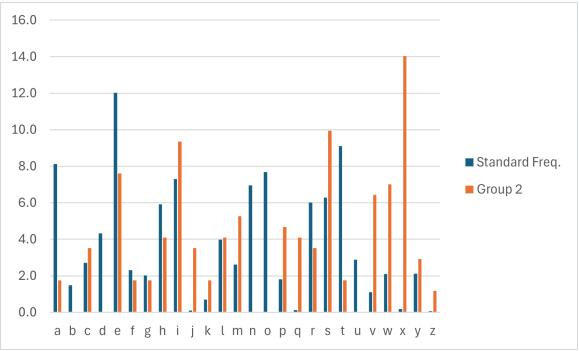


Letter Group 2



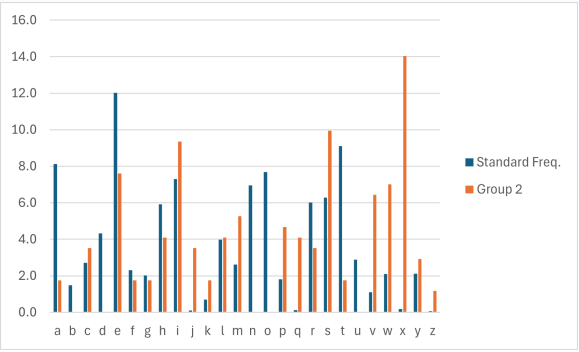
- Each group has been shifted by the same value: a Caesar cipher.

Letter Group 2



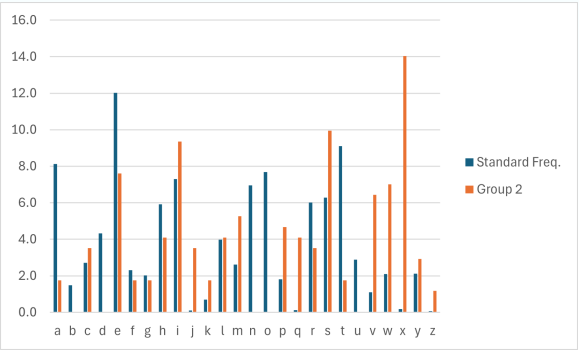
- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.

Letter Group 2



- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.
- There looks to be a gap like before from s to x, but the gap is 5 so can't be the gap from a to e.

Letter Group 2



- Each group has been shifted by the same value: a Caesar cipher.
- The charts will look the same, just shifted by a number of places.
- There looks to be a gap like before from `s` to `x`, but the gap is 5 so can't be the gap from `a` to `e`.
- Instead we can choose the gap `e` to `i` and deduce that the likely shift is `a` to `e`: shift value 4.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19,

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4,

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.
  - Group 5: shift 14,

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.
  - Group 5: shift 14, key letter `o`.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.
  - Group 5: shift 14, key letter `o`.
  - Group 6: shift 17.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.
  - Group 5: shift 14, key letter `o`.
  - Group 6: shift 17. key letter `r`.

Other Letter Groups

- We can continue this analysis for each of the groups. The key length is 6 so there will be six groups to consider.
- We make the following guesses:
  - Group 1: shift 12, key letter `m`.
  - Group 2: shift 4, key letter `e`.
  - Group 3: shift 19, key letter `t`.
  - Group 4: shift 4, key letter `e`.
  - Group 5: shift 14, key letter `o`.
  - Group 6: shift 17. key letter `r`.
- So the keyword appears to be `meteor` and we can then attempt to decrypt the text.

noonewouldhavebelievedinthelastyearsofthenineteenthcenturythatthisworldw
asbeingwatchedkeenlyandcloselybyintelligencesgreaterthanmansandyetasmortalashi
wnthatasmenbusiedthemselvesabouttheirvariousconcernstheywerescrutinisedandstud
dperhapsalmostasnarrowlyasamanwithamicroscopemightscrutinisethetransientcreatu
sthatswarmandmultiplyinadropofwaterwithinfinitecomplacencymenwenttoandfroovert
sglobeabouttheirlittleaffairssereneintheirassuranceoftheirempireovermatteritis
ssiblethattheinfusoriaunderthemicroscopedothesamenoonegaveathoughttotheolderwo
dsofspaceassourcesofhumandangerorthoughtofthemonlytodismisstheideaoflifeuponth
asimpossibleorimprobableitiscurioustorecallsomeofthementalhabitsofthosedeparte
aysatmostterrestrialmenfanciedtheremightbeothermenuponmarsperhapsinferiortothe
elvesandreadytowelcomeamissionaryenterpriseyetacrossthegulfofspacemindsthatare
ourmindsasoursaretothoseofthebeaststhatperishintellectsvastandcoolandunsympath
icregardedthisearthwithenviouseyesandslowlyandsurelydrewtheirplansagainstus

noone would have believed in the last years of the nineteenth century that this world was being watched keenly and closely by intelligences greater than mans and yet as mortal as his own that as men busied themselves about their various concerns they were scrutinised and studied perhaps almost as narrowly as a man with a microscope might scrutinise the transient creatures that swarm and multiply in a drop of water with infinite complacency men went to and fro over this globe about their little affairs serene in their assurance of their empire over matter it is possible that the infusoria under the microscope do the same noone gave a thought to the older worlds of space as sources of human danger or thought of them only to dismiss the idea of life upon them as impossible or improbable it is curious to recall some of the mental habits of those departed days at most terrestrial men fancied there might be other men upon mars perhaps inferior to themselves and ready to welcome a missionary enterprise yet across the gulf of space minds that are to our minds as ours are to those of the beasts that perish intellects vast and cool and unsympathetic regarded this earth with envious eyes and slowly and surely drew their plans against us

Finding the Key Length

- Common letter groupings like '`the`' will often get encrypted using the same key letters.

Finding the Key Length

- Common letter groupings like '`the`' will often get encrypted using the same key letters.
- This gives repeated strings of letters in the ciphertext.

Finding the Key Length

- Common letter groupings like '`the`' will often get encrypted using the same key letters.
- This gives repeated strings of letters in the ciphertext.
- This forms the basis of a **Kasiski attack**.

Finding the Key Length

- Common letter groupings like '`the`' will often get encrypted using the same key letters.
- This gives repeated strings of letters in the ciphertext.
- This forms the basis of a **Kasiski attack**.
- Longer messages are more likely to yield to such an attack as there will be more repeated segments.

Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

Breaking Vigenère

- The sequence `XAIA` is repeated in the ciphertext and the two sequences are 288 letters apart.

Breaking Vigenère

- The sequence `XAIA` is repeated in the ciphertext and the two sequences are 288 letters apart.
- This length is called the **interval**.

Breaking Vigenère

- The sequence `XAIA` is repeated in the ciphertext and the two sequences are 288 letters apart.
- This length is called the **interval**.
- We break this interval into its prime factors:

$$288 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3.$$

Breaking Vigenère

- The sequence `XAIA` is repeated in the ciphertext and the two sequences are 288 letters apart.
- This length is called the **interval**.
- We break this interval into its prime factors:

$$288 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3.$$

- The key length could be 2, 3, 4, 6, 8, 9, 12, 18, 24, 32, 36, 48, 72, 96, 133, or 288.

Breaking Vigenère

- The sequence `XAIA` is repeated in the ciphertext and the two sequences are 288 letters apart.
- This length is called the **interval**.
- We break this interval into its prime factors:

$$288 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3.$$

- The key length could be 2, 3, 4, 6, 8, 9, 12, 18, 24, 32, 36, 48, 72, 96, 133, or 288.
- We've narrowed it down, but that's still a lot of options.

Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

Breaking Vigenère

- The sequence `FLX` is repeated in the ciphertext and the two sequences are 60 letters apart.

Breaking Vigenère

- The sequence `FLX` is repeated in the ciphertext and the two sequences are 60 letters apart.
- We break this interval into its prime factors:

$$60 = 2 \times 2 \times 3 \times 5.$$

Breaking Vigenère

- The sequence `FLX` is repeated in the ciphertext and the two sequences are 60 letters apart.
- We break this interval into its prime factors:

$$60 = 2 \times 2 \times 3 \times 5.$$

- The key length could be 2, 3, 4, 5, 6, 10, 12, 15, 30, or 60.

Breaking Vigenère

- The sequence `FLX` is repeated in the ciphertext and the two sequences are 60 letters apart.
- We break this interval into its prime factors:

$$60 = 2 \times 2 \times 3 \times 5.$$

- The key length could be 2, 3, 4, 5, 6, 10, 12, 15, 30, or 60.
- Some of these options match what we had before.

Breaking Vigenère

- The sequence `FLX` is repeated in the ciphertext and the two sequences are 60 letters apart.
- We break this interval into its prime factors:

$$60 = 2 \times 2 \times 3 \times 5.$$

- The key length could be 2, 3, 4, 5, 6, 10, 12, 15, 30, or 60.
- Some of these options match what we had before.
- We repeat this with other sequences.

Breaking Vigenère

ZSHRSNAYEHVRHIUIZZQZXHWEFLXPOJFCXEFJAJMLSEURXXSVZXAGSEFYKCHYMXMLWJISKPRN
MWUIWESATXQYQHDISEXCTRRTXSLIZPNCBRHVXPBKSEOILKFVMXXVHYMRFEBJMRWCSKMWFSFK
MPTWVZESPRHYMXTWAVZFNWWVPXAIAJQPOIGRNSNXHYQMKZOIUSNWQFZGXVBJFLXCKVDILGFL
FMGMGVPEGHGKGHBIRGQVAEDJMPFSGKMWGEFIAAECOJMQTRKZFLTQWTDSLGCGQQBKVKEGKYHZ
ZMLIHYQXKEBJUIGXQIQEMYFVEXAEHJIEKQOEPQNPHZBPRMBRPVHTCWIEMIFNUXAMBWURBXST
AQIPOTQRVCAVZAXRHKAEGHTIASOIFKTMLKZFNITFCLFXAIWIXMMXZVMJYEWIEWXVSEQMGXVV
UVTWGLDEGGSFRXAIWIQQIMFVAZXVARFXXVWKUWISGJUFEIHYMXMLSZZJNWCIUENRRVDXAIAZ
OVHWQFBIWSHYQWTQSEASGIURHITXVFGKAXHFFLXSZUQVPSFCPWHJGGMGXEGJAYKGSJAJAYAR
ZHTRUVDSKXVFGKAXCWFLXQCEXCMSRZEQBWGKTIBHSRAJEMTVGTHRHYQQTWWDBSLWWSXIHVWD
BVHFOSXIBXWJOYKMCLEXHVSTMPEWCDQSYXVVYIGXOCTEUMHJAJMLCJQHXTOIFIWHOPEEMQCJ
FXXVFVEXKMOCYIGJOEOMXHHYQVXQWXTXUICKTIKQSEGTHRARDWIIFYMTLMBWQVBSFKAXAIAJ
QPOIGRZHKIOUKXHASCOSFIODUWLMCEMVRIBKQVIVWJQCXXOTDSLWHYQKNPTFRWIEQVYMGHGK
TEMEFVFSHYFDURWWOJAYKWOIQXHXVFEIHJHYQFXEGKEXAEHGQVBWVZZXXPZVOXLZOJFEGHQF
APTRRLZWRQDRFLXXWTDIZEFUQHMLWJQEKXVNUXAIBMUSNWSPQWTRRJXSPPMRZHLYFVXCWVSN
FLXMFGXEGWOXMMGWHLE

Breaking Vigenère

- The sequence `HYQ` is repeated in the ciphertext and the two sequences are 108 letters apart.

Breaking Vigenère

- The sequence `HYQ` is repeated in the ciphertext and the two sequences are 108 letters apart.
- We break this interval into its prime factors:

$$108 = 2 \times 2 \times 3 \times 3 \times 3.$$

Breaking Vigenère

- The sequence `HYQ` is repeated in the ciphertext and the two sequences are 108 letters apart.
- We break this interval into its prime factors:

$$108 = 2 \times 2 \times 3 \times 3 \times 3.$$

- The key length could be 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, or 108.

Breaking Vigenère

- The sequence `HYQ` is repeated in the ciphertext and the two sequences are 108 letters apart.
- We break this interval into its prime factors:

$$108 = 2 \times 2 \times 3 \times 3 \times 3.$$

- The key length could be 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, or 108.
- Some of these options again match what we had before.

Breaking Vigenère

- The sequence `HYQ` is repeated in the ciphertext and the two sequences are 108 letters apart.
- We break this interval into its prime factors:

$$108 = 2 \times 2 \times 3 \times 3 \times 3.$$

- The key length could be 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, or 108.
- Some of these options again match what we had before.
- We repeat this again with other sequences.

Breaking Vigenère

sequence	interval	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
XAIA	288	X	X	X		X		X	X			X				X
FLX	60	X	X	X	X	X				X		X			X	
HYQ	108	X	X	X		X			X			X				
XVF	54	X	X	X		X			X			X				
YMX	96	X	X	X		X		X				X				X
KAX	54	X	X	X		X			X			X				
FXXV	258	X	X			X										

Breaking Vigenère

- It is possible that some repeated sequences are just due to coincidence.

Breaking Vigenère

- It is possible that some repeated sequences are just due to coincidence.
- With longer sequences, this becomes less likely.

Breaking Vigenère

- It is possible that some repeated sequences are just due to coincidence.
- With longer sequences, this becomes less likely.
- If we analyse the factors in the table, the obvious candidates for key lengths are 2, 3, 4, and 6.

Breaking Vigenère

- It is possible that some repeated sequences are just due to coincidence.
- With longer sequences, this becomes less likely.
- If we analyse the factors in the table, the obvious candidates for key lengths are 2, 3, 4, and 6.
- Key lengths of 2, 3 or 4 are quite short, so we rule them out. (We may have to come back to them.)

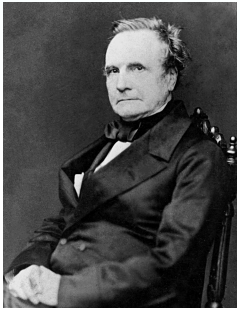
Breaking Vigenère

- It is possible that some repeated sequences are just due to coincidence.
- With longer sequences, this becomes less likely.
- If we analyse the factors in the table, the obvious candidates for key lengths are 2, 3, 4, and 6.
- Key lengths of 2, 3 or 4 are quite short, so we rule them out. (We may have to come back to them.)

Breaking Vigenère

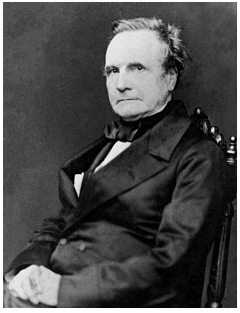
- It is possible that some repeated sequences are just due to coincidence.
- With longer sequences, this becomes less likely.
- If we analyse the factors in the table, the obvious candidates for key lengths are 2, 3, 4, and 6.
- Key lengths of 2, 3 or 4 are quite short, so we rule them out. (We may have to come back to them.) The key length is likely to be 6 and as we found out, the actual keyword was `meteor`.

Who broke the unbreakable cipher?



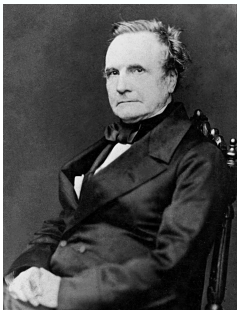
- Our method is known as a Kasiski attack, but somebody else had got there first.

Who broke the unbreakable cipher?



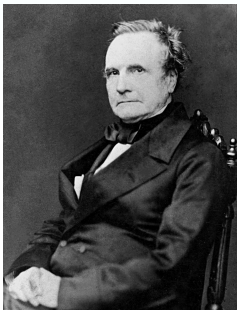
- Our method is known as a Kasiski attack, but somebody else had got there first.
- German cryptographer and archaeologist Friedrick Kasiski attacked the problem in 1863.

Who broke the unbreakable cipher?



- Our method is known as a Kasiski attack, but somebody else had got there first.
- German cryptographer and archaeologist Friedrick Kasiski attacked the problem in 1863.
- But Charles Babbage had cracked it in 1854. The British government wanted to keept it secret in the Crimean War.

Who broke the unbreakable cipher?



- Our method is known as a Kasiski attack, but somebody else had got there first.
- German cryptographer and archaeologist Friedrick Kasiski attacked the problem in 1863.
- But Charles Babbage had cracked it in 1854. The British government wanted to keept it secret in the Crimean War.
- We know Babbage better as being the originator of the programmable computer, having designed the Analytical and Differences Engines.

Tutorials

In the tutorial this week we will:

- Create a spreadsheet to perform Vigenère encryption.
- Use a premade spreadsheet to perform a Kasiski-style attack on Vigenère encryption.