The Vigenère Cipher

October 25, 2021

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14

The Vigenère Cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14
Shift 6th letter by 6, etc.

The Vigenère Cipher

Key: A word or phrase. Example: *dog = (3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14
Shift 6th letter by 6, etc.

Jacob Prinz is a Physics Major
Jacob Prinz isaPh ysics Major

encrypts to

The Vigenère Cipher

Key: A word or phrase. Example: *dog = (3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14
Shift 6th letter by 6, etc.

Jacob Prinz is a Physics Major
Jacob Prinz isaPh ysics Major

encrypts to

MOIRP VUWTC WYDDN BGOFG SDXUU

The Vigenère Cipher

Key: $k = (k_1, k_2, \ldots, k_n)$.
Encrypt (all arithmetic is mod 26)

$$Enc(m_1, m_2, \ldots, m_N) =$$

$$m_1 + k_1, m_2 + k_2, \ldots, m_n + k_n,$$

$$m_{n+1} + k_1, m_{n+2} + k_2, \ldots, m_{n+n} + k_n,$$

$$\ldots$$

Decrypt Decryption just reverses the process

Three Kinds of Vigenère Ciphers

The following three slides give three kinds of Vig Ciphers. It is a rough way to divide up types of Vig ciphers. There will be some that are not quite in any category.

VIG ONE: Standard Vigenère Ciphers

The key is a sentence or paragraph in English. Memorable and not to long. For example, the following could be the key:

VIG ONE: Standard Vigenère Ciphers

The key is a sentence or paragraph in English. Memorable and not to long. For example, the following could be the key:

When the TV game show Jeopardy had the topic CHEMISTRY they had the questions read by, not a famous chemist, but by Bryan Cranston who played a chemist on Breaking Bad. Why? Because there are no famous living chemists. This is sad!

VIG ONE: Standard Vigenère Ciphers

The key is a sentence or paragraph in English. Memorable and not to long. For example, the following could be the key:

When the TV game show Jeopardy had the topic CHEMISTRY they had the questions read by, not a famous chemist, but by Bryan Cranston who played a chemist on Breaking Bad. Why? Because there are no famous living chemists. This is sad!

We will be studying this type of Vig cipher today.

VIG TWO: The Vig-Book Cipher

The key is an entire book that Alice and Bob both have. Has to be the same edition!

VIG TWO: The Vig-Book Cipher

The key is an entire book that Alice and Bob both have. Has to be the same edition!

The key that Alice tells Bob can still be short since books have title and authors and edition numbers that identify them.

VIG TWO: The Vig-Book Cipher

The key is an entire book that Alice and Bob both have. Has to be the same edition!

The key that Alice tells Bob can still be short since books have title and authors and edition numbers that identify them.

Alice can say to Bob:

VIG TWO: The Vig-Book Cipher

The key is an entire book that Alice and Bob both have. Has to be the same edition!

The key that Alice tells Bob can still be short since books have title and authors and edition numbers that identify them.

Alice can say to Bob:

A Student's Guide to Coding and Information theory by Moser and Chen, 2nd edition.

VIG TWO: The Vig-Book Cipher

The key is an entire book that Alice and Bob both have. Has to be the same edition!

The key that Alice tells Bob can still be short since books have title and authors and edition numbers that identify them.

Alice can say to Bob:

A Student's Guide to Coding and Information theory by Moser and Chen, 2nd edition.

This is called **The Vig-Book Cipher**. We will touch on it briefly later.

VIG THREE: The One Time Pad

The key is a very long random string of letters. Note that the key is completely random, so not memorable at all. Alice would give Bob that very long string, which is awkward.

VIG THREE: The One Time Pad

The key is a very long random string of letters. Note that the key is completely random, so not memorable at all. Alice would give Bob that very long string, which is awkward.

This is called **The One-Time Pad**. We will study it later.

VIG THREE: The One Time Pad

The key is a very long random string of letters. Note that the key is completely random, so not memorable at all. Alice would give Bob that very long string, which is awkward.

This is called **The One-Time Pad**. We will study it later.

It is usually done with alphabet $\{0, 1\}$ or $\{0, \ldots, 9\}$, not $\{a, \ldots, z\}$.

Crypto Dilemma and what Amateur's Have Done

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

In an earlier era many amateurs came up with cryptosystems that they thought were unbreakable. Their fallacies:

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

In an earlier era many amateurs came up with cryptosystems that they thought were unbreakable. Their fallacies:

1. Their systems where impossible to use.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

In an earlier era many amateurs came up with cryptosystems that they thought were unbreakable. Their fallacies:

1. Their systems where impossible to use.
2. Their systems were only hard to break on short ciphers.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

In an earlier era many amateurs came up with cryptosystems that they thought were unbreakable. Their fallacies:

1. Their systems where impossible to use.
2. Their systems were only hard to break on short ciphers.
3. They assumed that the only way to break it was similar to how it was created. Example: There are 26! possibly general sub ciphers, so unbreakable.

Crypto Dilemma and what Amateur's Have Done

- Vig ONE: easy to use, but as we will see, Easy to Break.
- One-time-Pad: hard to use, but as we will see, Hard to Break.

This is the **Cryptographers Dilemma.** How to make a system that is easy for Alice and Bob to **use** but hard for Eve to **break**.

In an earlier era many amateurs came up with cryptosystems that they thought were unbreakable. Their fallacies:

1. Their systems where impossible to use.
2. Their systems were only hard to break on short ciphers.
3. They assumed that the only way to break it was similar to how it was created. Example: There are 26! possibly general sub ciphers, so unbreakable. NOT!

Our Study of VIG ONE

- Size of key space?

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.
  - If Eve knows that Alice and Bob are fans of American History and suspects they use phrases about it (e.g., names of Vice Presidents) brute-force is even more feasible.

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.
  - If Eve knows that Alice and Bob are fans of American History and suspects they use phrases about it (e.g., names of Vice Presidents) brute-force is even more feasible.
- Is the Vigenère cipher secure?

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.
  - If Eve knows that Alice and Bob are fans of American History and suspects they use phrases about it (e.g., names of Vice Presidents) brute-force is even more feasible.
- Is the Vigenère cipher secure?
- Believed secure for many years...

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.
  - If Eve knows that Alice and Bob are fans of American History and suspects they use phrases about it (e.g., names of Vice Presidents) brute-force is even more feasible.
- Is the Vigenère cipher secure?
- Believed secure for many years...
- Might not have even been secure then...

Our Study of VIG ONE

- Size of key space?
  - If keys are $\leq$ 20-char then key space size $\sim 26^{20}$.
  - If key can be **anything** then brute-force search is infeasible.
  - If key is an English Sentence, Brute-force might be feasible.
  - If Eve knows that Alice and Bob are fans of American History and suspects they use phrases about it (e.g., names of Vice Presidents) brute-force is even more feasible.
- Is the Vigenère cipher secure?
- Believed secure for many years...
- Might not have even been secure then...
- History of Cryptography is hard since, unlike most science, people can discover things and NOT brag about it.

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.
For $0 \leq i \leq L-1$, letters in pos $\equiv i \pmod{L}$ – same shift.
Look for a sequence of (say) 3-letters to appear (say) 4 times.

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.
For $0 \leq i \leq L-1$, letters in pos $\equiv i \pmod{L}$ – same shift.
Look for a sequence of (say) 3-letters to appear (say) 4 times.

Example: **aiq** appears in the
57-58-59th slot 87-88-89th slot 102-103-104th slot
162-163-164th slot

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.
For $0 \leq i \leq L-1$, letters in pos $\equiv i \pmod{L}$ – same shift.
Look for a sequence of (say) 3-letters to appear (say) 4 times.

Example: **aiq** appears in the
57-58-59th slot 87-88-89th slot 102-103-104th slot
162-163-164th slot

Important: Very likely that **aiq** encrypted **the same** 3-letter sequence and hence the **length** of the key is a divisor of
87-57=30 102-87=15 162-102=60
The only possible L's are 1,3,5,15.

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.
For $0 \leq i \leq L-1$, letters in pos $\equiv i \pmod{L}$ – same shift.
Look for a sequence of (say) 3-letters to appear (say) 4 times.

Example: **aiq** appears in the
57-58-59th slot 87-88-89th slot 102-103-104th slot
162-163-164th slot

Important: Very likely that **aiq** encrypted **the same** 3-letter sequence and hence the **length** of the key is a divisor of
87-57=30 102-87=15 162-102=60
The only possible L's are 1,3,5,15.

Good Enough: We got the key length down to a small finite set.

Important Point About Letter Freq (I)

In an English text T of length N, where N is large:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters have frequencies that are true for all texts.

Important Point About Letter Freq (I)

In an English text T of length N, where N is large:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters have frequencies that are true for all texts.

In an English text T of length N, where N is large and $i \ll N$, then if you take **every ith letter of T**:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- have the other letters same frequencies as normal texts.

Important Point About Letter Freq (II)

If T is a text of normal English then $f_T \cdot f_E \sim 0.065$.

Important Point About Letter Freq (II)

If T is a text of normal English then $f_T \cdot f_E \sim 0.065$.

Hence, if T is a text of normal English then $f_T \cdot f_T \sim 0.065$.

Important Point About Letter Freq (II)

If T is a text of normal English then $f_T \cdot f_E \sim 0.065$.

Hence, if T is a text of normal English then $f_T \cdot f_T \sim 0.065$.

Very Important If T is a **shifted text of normal English** then $f_T \cdot f_T \sim f_E \cdot f_E \sim 0.065$.

Important Point About Letter Freq (II)

If T is a text of normal English then $f_T \cdot f_E \sim 0.065$.

Hence, if T is a text of normal English then $f_T \cdot f_T \sim 0.065$.

Very Important If T is a **shifted text of normal English** then $f_T \cdot f_T \sim f_E \cdot f_E \sim 0.065$.

Contrast If T is not normal English or a shift of normal English then $f_T \cdot f_T$ is probably low.

Important Point About Letter Freq (II)

If T is a text of normal English then $f_T \cdot f_E \sim 0.065$.

Hence, if T is a text of normal English then $f_T \cdot f_T \sim 0.065$.

Very Important If T is a **shifted text of normal English** then $f_T \cdot f_T \sim f_E \cdot f_E \sim 0.065$.

Contrast If T is not normal English or a shift of normal English then $f_T \cdot f_T$ is probably low.

Sum Up Point

- If T is English or shifted-English then $f_T \cdot f_T \sim 0.065$ large.
- If T is not English nor shifted-English then $f_T \cdot f_T$ is prob small.

We Can Use This

We think that Key Length is (say) 10

We Can Use This

We think that Key Length is (say) 10

How to test this? Discuss

We Can Use This

We think that Key Length is (say) 10

How to test this? Discuss

1. Let T_0 be the letters in T in spots 0, 10, 20, 30, ...

We Can Use This

We think that Key Length is (say) 10

How to test this? Discuss

1. Let T_0 be the letters in T in spots 0, 10, 20, 30, ...
2. If $f_{T_0} \cdot f_{T_0}$ is large then key length probably IS 10 (or a divisor of 10).

We Can Use This

We think that Key Length is (say) 10

How to test this? Discuss

1. Let T_0 be the letters in T in spots 0, 10, 20, 30, ...
2. If $f_{T_0} \cdot f_{T_0}$ is large then key length probably IS 10 (or a divisor of 10).
3. If $f_{T_0} \cdot f_{T_0}$ is small then key length probably not 10.

Next slide generalizes this.

Testing if Key Length is L

Our question T is ciphertext coded with Vig Cipher. Eve thinks the key length is L. Let S be **every Lth letter of T**. SO

$$S = T(1)T(L+1)T(2L+1)\cdots T(NL+1)$$

Testing if Key Length is L

Our question T is ciphertext coded with Vig Cipher. Eve thinks the key length is L. Let S be **every Lth letter of T**. SO

$$S = T(1)T(L+1)T(2L+1)\cdots T(NL+1)$$

- If keylength is L then S is a shift of every Lth character from some English Text. Hence $f_S \cdot f_S \sim 0.065$.

Testing if Key Length is L

Our question T is ciphertext coded with Vig Cipher. Eve thinks the key length is L. Let S be **every Lth letter of T**. SO

$$S = T(1)T(L+1)T(2L+1)\cdots T(NL+1)$$

- If keylength is L then S is a shift of every Lth character from some English Text. Hence $f_S \cdot f_S \sim 0.065$.
- If keylength is not L then S is a ... a real mess!! $f_S \cdot f_S$ will be small.

Upshot We have a test whether some text is from the shift-cipher or not. We will use it on the every-Lth-letter text of T.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.
- Compute $Q = f_S \cdot f_S$.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.
- Compute $Q = f_S \cdot f_S$.
- If $Q \approx 0.065$ then YES L is key length.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.
- Compute $Q = f_S \cdot f_S$.
- If $Q \approx 0.065$ then YES L is key length.
- If Q much less than 0.065 then NO L is not key length.

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.
- Compute $Q = f_S \cdot f_S$.
- If $Q \approx 0.065$ then YES L is key length.
- If Q much less than 0.065 then NO L is not key length.
- One of these two will happen:

Cracking Vig: Step One-Find Keylength (cont)

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream S of every Lth character.
- Find the frequencies of that stream, f_S.
- Compute $Q = f_S \cdot f_S$.
- If $Q \approx 0.065$ then YES L is key length.
- If Q much less than 0.065 then NO L is not key length.
- One of these two will happen:
- Just to make sure, check another stream.

Another Way To Find Keylength

We presented Method ONE:

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Or could try all key lengths up to a certain length,
Method TWO:

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Or could try all key lengths up to a certain length,
Method TWO:

1. Let $K = \{1, \ldots, 100\}$ (I am assuming key length ≤ 100).

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Or could try all key lengths up to a certain length,
Method TWO:

1. Let $K = \{1, \ldots, 100\}$ (I am assuming key length ≤ 100).
2. Test $L \in K$ for key length until find one that works.

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Or could try all key lengths up to a certain length,
Method TWO:

1. Let $K = \{1, \ldots, 100\}$ (I am assuming key length ≤ 100).
2. Test $L \in K$ for key length until find one that works.

Note With modern computers use Method TWO. In the pre-computation era Method ONE was used.

Another Way To Find Keylength

We presented Method ONE:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Or could try all key lengths up to a certain length,
Method TWO:

1. Let $K = \{1, \ldots, 100\}$ (I am assuming key length ≤ 100).
2. Test $L \in K$ for key length until find one that works.

Note With modern computers use Method TWO. In the pre-computation era Method ONE was used.
Question Computers reduce the need for cleverness. Is this good or bad?

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.
- **Important:** Letter Freq still holds if you look at every Lth letter!

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.
- **Important:** Letter Freq still holds if you look at every Lth letter!

Step Two:

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.
- **Important:** Letter Freq still holds if you look at every Lth letter!

Step Two:

1. Separate text T into L streams depending on position mod L.

Cracking the Vig cipher: Step Two-Freq Anal

After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.
- **Important:** Letter Freq still holds if you look at every Lth letter!

Step Two:

1. Separate text T into L streams depending on position mod L.
2. For each steam try every shift and use **Is English** to determine which shift is correct.

Cracking the Vig cipher: Step Two-Freq Anal

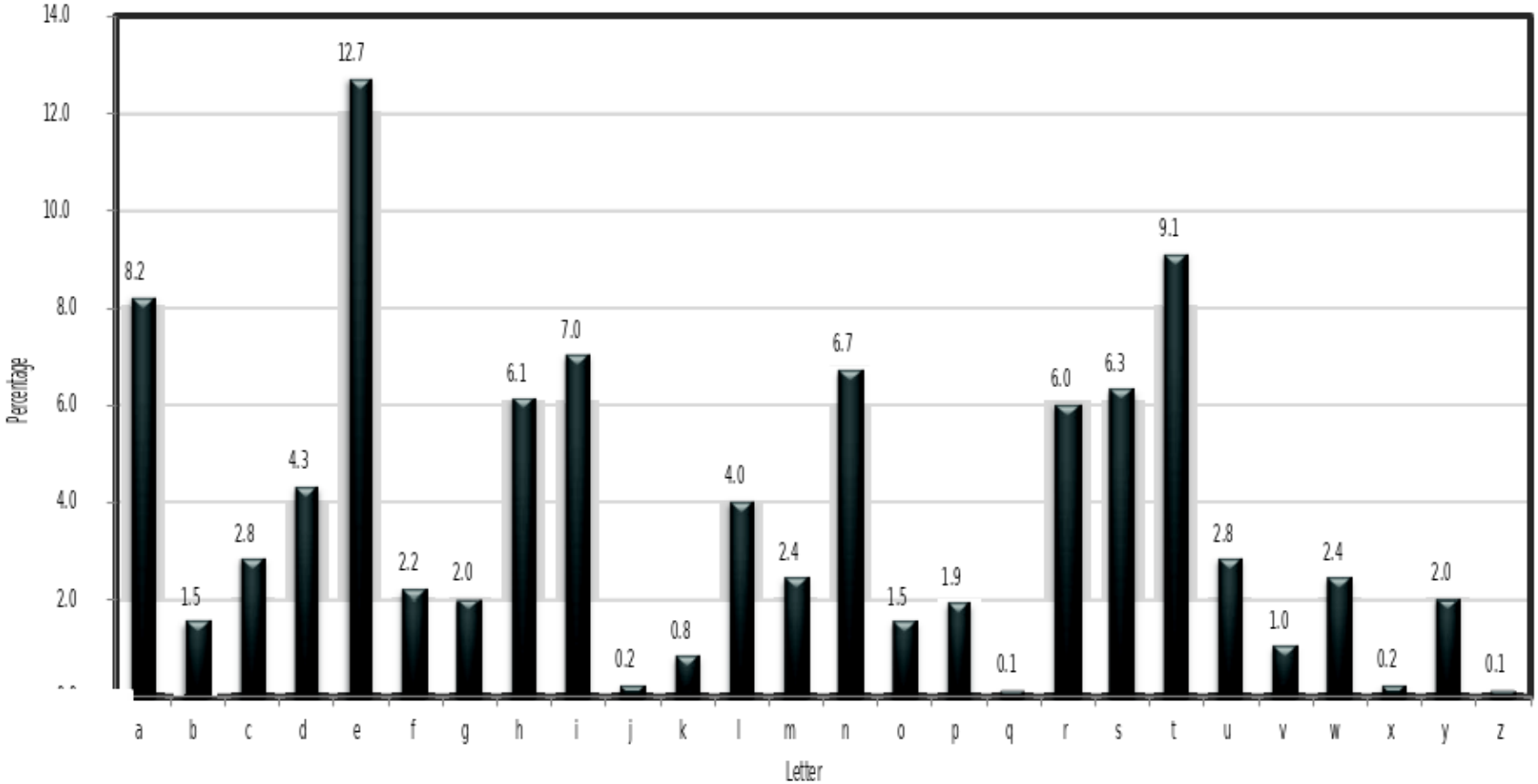
After Step One we have the key length L. Note:

- Every L^{th} character is **encrypted** using the same shift.
- **Important:** Letter Freq still holds if you look at every Lth letter!

Step Two:

1. Separate text T into L streams depending on position mod L.
2. For each steam try every shift and use **Is English** to determine which shift is correct.
3. You now know all shifts for all positions. Decrypt!

Using Plaintext Letter Frequencies



Vig-Book Cipher

October 25, 2021

Vig-Book Cipher

A student said:

Let's use Vig cipher with a book for the key

Is it a good idea? **Discuss**

Vig-Book Cipher

A student said:

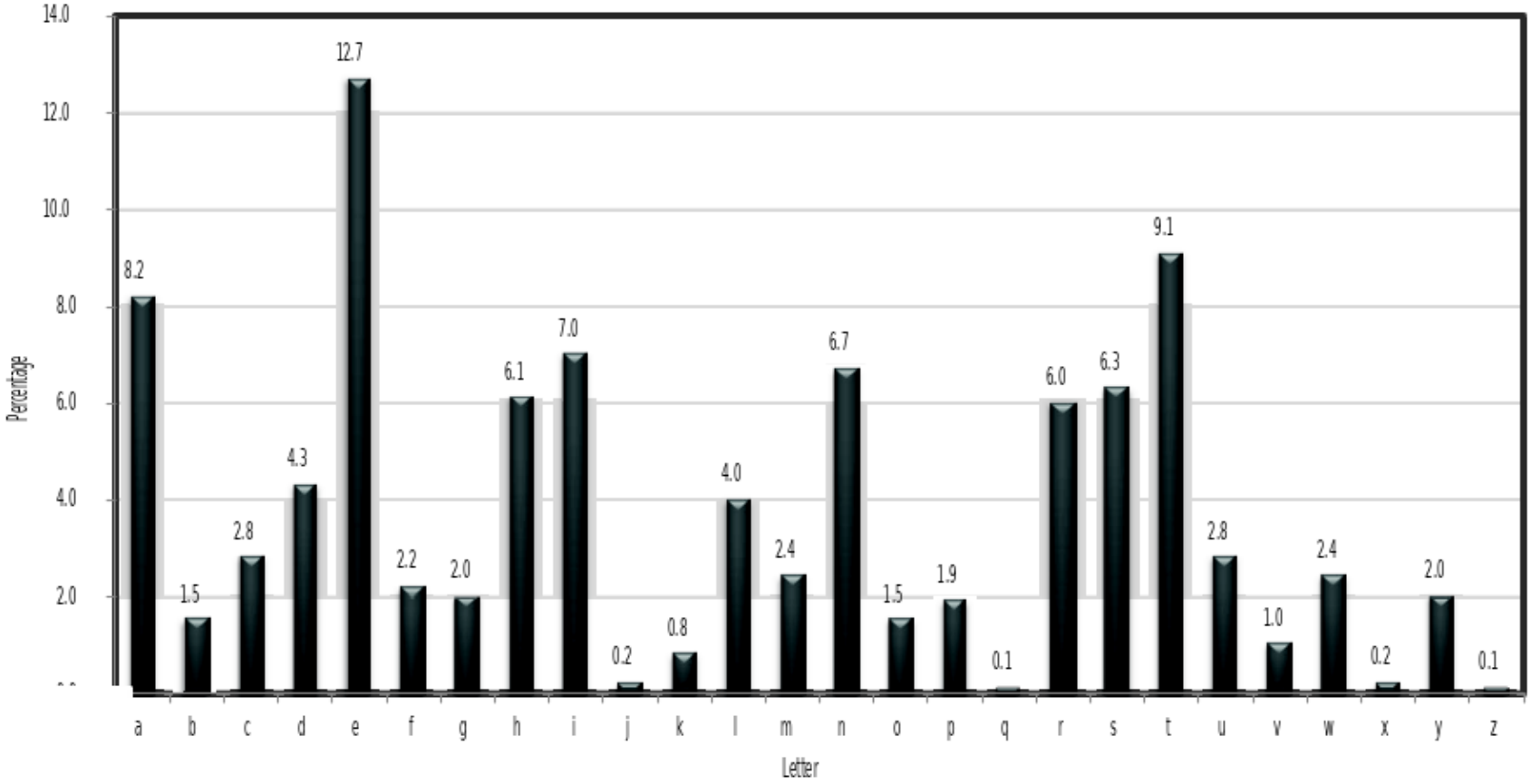
Let's use Vig cipher with a book for the key

Is it a good idea? **Discuss**

1. Before modern computer era: YES.
2. Now. NO.

How to Crack the Vig-Book Cipher

Key: Both Key and Text have the English Lang Frequencies.



How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.
3. (a, d): Hmm, seems more likely than (z, e).

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.
3. (a, d): Hmm, seems more likely than (z, e).
4. Can rank which are more likely (e.g., add or mult the freqs).

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.
3. (a, d): Hmm, seems more likely than (z, e).
4. Can rank which are more likely (e.g., add or mult the freqs).
5. Can then use adj letters and freq of adj pairs, and rank them.

How to Crack the Vig-Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.
3. (a, d): Hmm, seems more likely than (z, e).
4. Can rank which are more likely (e.g., add or mult the freqs).
5. Can then use adj letters and freq of adj pairs, and rank them.
6. Triples. Etc.

Vig-Book Cipher was Really Used

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**.

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book **Germany and the Germans**.

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book **Germany and the Germans**. Really!

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book **Germany and the Germans**. Really!

Were these good choices?

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book **Germany and the Germans**. Really!

Were these good choices? NO.

Vig-Book Cipher was Really Used

1. Benedict Arnold used the Vig-Book Cipher with the book **Commentaries on the laws of England**. Really!
2. In WW I, Germany and a group in India that wanted independence from England, communicated using the Vig-Book Cipher. They used the book **Germany and the Germans**. Really!

Were these good choices? NO. They are books Eve might guess.

Bill Should Not Use...

Bill Should Not Use. . .

Problems with a Point

Ever notice how civilians (that is non-math people) use math words badly? Ever notice how sometimes you know a math statement is false (or not known) since if it was true you would know it?

Each chapter of this book makes a point like those above and then illustrates the point by doing some real mathematics.

This book gives readers valuable information about how mathematics and theoretical computer science work, while teaching them some actual mathematics and computer science through examples and exercises. Much of the mathematics could be understood by a bright high school student. The points made can be understood by anyone with an interest in math, from the bright high school student to a Field's medal winner.

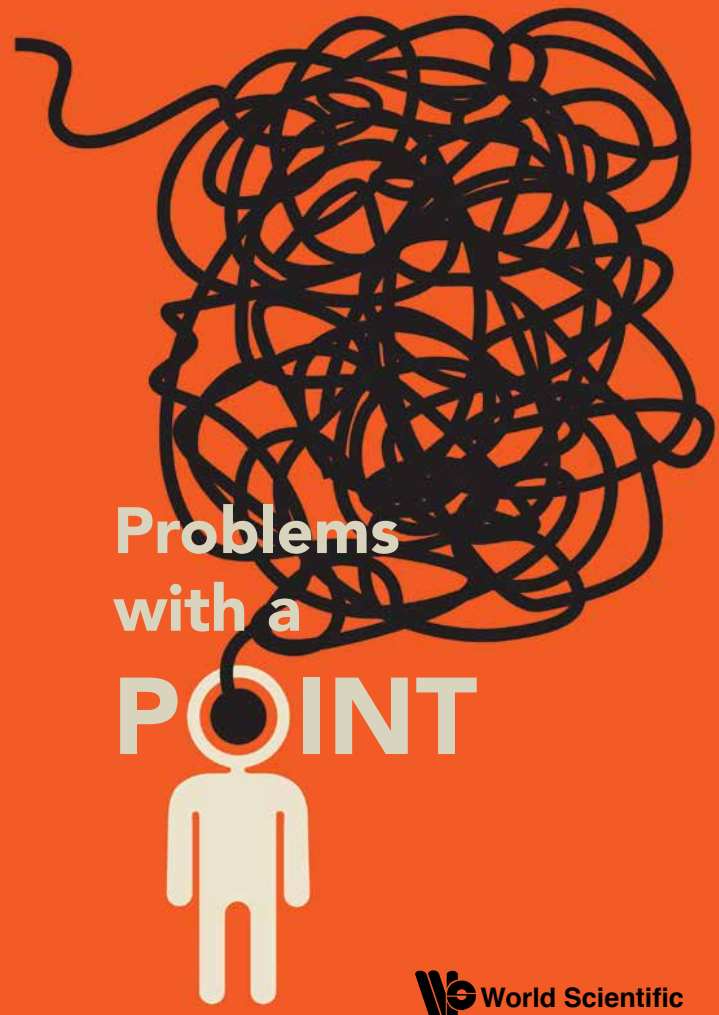
World Scientific
www.worldscientific.com
11261 hc

ISBN 978-981-3279-72-8
9 789813 279728

Problems with a POINT

Gasarch
Kruskal

William Gasarch • Clyde Kruskal



Problems with a POINT

World Scientific

Would make a Good Ugrad Project

Cracking the book cipher would make a good ugrad project.

Vig Cipher with Key Longer Than Message

The Vig-Book Cipher IS Vig Cipher with Key longer than message.

1. **Weakness:** Key is English Phrase, so has freq patterns.
2. How can we strengthen?

Vig Cipher with Key Longer Than Message

The Vig-Book Cipher IS Vig Cipher with Key longer than message.

1. **Weakness:** Key is English Phrase, so has freq patterns.
2. How can we strengthen?
3. Make Key Truly Random. This is the one-time pad which we study later.