BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

PIN Numbers

September 27, 2020

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known. **NO** - it premeired in 2018.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known. **NO** - it premeired in 2018.

Eve is tracking an assasin who is a psychopath. Here is some good advice:

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known. **NO** - it premeired in 2018.

Eve is tracking an assasin who is a psychopath. Here is some good advice:

Eve to Psychopath You're a psychopath.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known. **NO** - it premeired in 2018.

Eve is tracking an assasin who is a psychopath. Here is some good advice:

Eve to Psychopath You're a psychopath.

Psychopath to Eve You should never call a psychopath a psychopath.

The TV Show Killing Eve: PIN numbers and...

Season one of **Killing Eve** was great. The rest... were not.

Eve works for MI-5.

Eve's pin number is 1-2-3-4. Gee, a spy should know better.

To be fair The show was made a while back before awareness of security was as well known. **NO** - it premeired in 2018.

Eve is tracking an assasin who is a psychopath. Here is some good advice:

Eve to Psychopath You're a psychopath.

Psychopath to Eve You should never call a psychopath a psychopath. It gets them angry.

Top 10 Pin Numbers

Write down a number you think will be in the top 20.

Top 10 Pin Numbers

Write down a number you think will be in the top 20.

Rank	PIN	Freq
1	1234	10.713%
2	1111	6.016%
3	0000	1.881%
4	1212	1.197%
5	7777	0.745%
6	1004	0.616%
7	2000	0.613%
8	4444	0.526%
9	2222	0.516%
10	6969	0.512%

Was your number in the top 10? Poll: 1 is YES, 2 is NO.

Top 10 Pin Numbers

Write down a number you think will be in the top 20.

Rank	PIN	Freq
1	1234	10.713%
2	1111	6.016%
3	0000	1.881%
4	1212	1.197%
5	7777	0.745%
6	1004	0.616%
7	2000	0.613%
8	4444	0.526%
9	2222	0.516%
10	6969	0.512%

Was your number in the top 10? Poll: 1 is YES, 2 is NO.

20% of all PIN's are of the form 19XX. Most Common:

Top 10 Pin Numbers

Write down a number you think will be in the top 20.

Rank	PIN	Freq
1	1234	10.713%
2	1111	6.016%
3	0000	1.881%
4	1212	1.197%
5	7777	0.745%
6	1004	0.616%
7	2000	0.613%
8	4444	0.526%
9	2222	0.516%
10	6969	0.512%

Was your number in the top 10? Poll: 1 is YES, 2 is NO.

20% of all PIN's are of the form 19XX. Most Common: 1984.

Next 10 Most Popular PIN Numbers

Next 10 Most Popular PIN Numbers

Rank	PIN	Freq
11	9999	0.451%
12	3333	0.419%
13	5555	0.395%
14	6666	0.391%
15	1122	0.366%
16	1313	0.304%
17	8888	0.303%
18	4321	0.293%
19	2001	0.290%
20	1010	0.285%

Was our number in spots 11-20? Raise hands.

Next 10 Most Popular PIN Numbers

Rank	PIN	Freq
11	9999	0.451%
12	3333	0.419%
13	5555	0.395%
14	6666	0.391%
15	1122	0.366%
16	1313	0.304%
17	8888	0.303%
18	4321	0.293%
19	2001	0.290%
20	1010	0.285%

Was our number in spots 11-20? Raise hands.

Least common PIN when article was written was 8068. So use?

Could not find when article was written—author uses year as PIN?

Other Ciphers That Were Actually Used

September 27, 2020

The Playfair Cipher

September 27, 2020

The Playfair Cipher: The Motivation

Let $\Sigma = \{a, \ldots, z\}$
Recall:

1. The cipher that picks a RANDOM bijection from Σ^2 to Σ^2 was never used since there was never a time when it was usable by AND hard to crack.
2. The 2×2 matrix cipher was a way to get a *random looking* function (maybe) that was EASY for Alice and Bob to compute. But alas, its very use of math made it crackable.
3. We need another way to EASILY specify a bijection Σ^2 to Σ^2.

The Playfair Cipher: The Key

We use $\Sigma = \{a, \ldots, z\} - \{j\}$. Need a square. If need to use j use an i.

Key is a word or phrase. Delete all repeats from it. We will use **Bill Gasarch** which becomes BILGASRCH. Use the key to start a 5×5 array of all of the letters

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

The Playfair Cipher: The First Case

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

Given a pair, what do you map it to? Start by finding the pair in the grid.

1) If the pair are NOT in the same row or column then look at rectangle formed and take other corners. EXAMPLE: Map *RA*:

I	L	G	A
R	C	H	D

RA maps to *ID*.

The Playfair Cipher: The Second and Third Cases

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

2) If pair is in SAME col then map down 1 (wrap around)

EXAMPLE: Map LC:

L
C
K
Q
X

LC maps to CK.

3) If pair is in SAME row then map right (wrap around).

The Playfair Cipher: What if Two in a Row?

What if message is **'Problems with a point' is a great book** .

The Playfair Cipher: What if Two in a Row?

What if message is **'Problems with a point' is a great book** .

What do do about the double letters **oo** ?

The Playfair Cipher: What if Two in a Row?

What if message is **'Problems with a point' is a great book** .

What do do about the double letters **oo** ?

Before coding put an x after the first letter of a double letter:

'Problems with a point' is a great boxok

The Playfair Cipher: What if Two in a Row?

What if message is **'Problems with a point' is a great book** .

What do do about the double letters **oo** ?

Before coding put an x after the first letter of a double letter:

'Problems with a point' is a great boxok

What if the message has an odd number of letters?

The Playfair Cipher: What if Two in a Row?

What if message is **'Problems with a point' is a great book** .

What do do about the double letters **oo** ?

Before coding put an x after the first letter of a double letter:

'Problems with a point' is a great boxok

What if the message has an odd number of letters?
Add an x to the end.

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.
2. When it was invented it was the first cipher to encrypt pairs by pairs (matrix cipher was 1929). It was uncrackable in the late 1800's. (See later comment on that.)

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.
2. When it was invented it was the first cipher to encrypt pairs by pairs (matrix cipher was 1929). It was uncrackable in the late 1800's. (See later comment on that.)
3. At first it was turned down by the British Government who thought it was too complicated:

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.
2. When it was invented it was the first cipher to encrypt pairs by pairs (matrix cipher was 1929). It was uncrackable in the late 1800's. (See later comment on that.)
3. At first it was turned down by the British Government who thought it was too complicated:
   P: I will demonstrate its ease of use by teaching it to 3 elementary school boys in less than an hour.

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.
2. When it was invented it was the first cipher to encrypt pairs by pairs (matrix cipher was 1929). It was uncrackable in the late 1800's. (See later comment on that.)
3. At first it was turned down by the British Government who thought it was too complicated:
   P: I will demonstrate its ease of use by teaching it to 3 elementary school boys in less than an hour.
   Officer: That may be, but I think diplomats would have a hard time with it.

The Playfair Cipher: Origin

1. Charles Wheatstone invented it in 1854. His friend Lyon Playfair advocated for its use and always gave Wheatstone credit (calling it **Wheatstone's Cipher**) but Playfair's name got attached to it anyway.
2. When it was invented it was the first cipher to encrypt pairs by pairs (matrix cipher was 1929). It was uncrackable in the late 1800's. (See later comment on that.)
3. At first it was turned down by the British Government who thought it was too complicated:
   P: I will demonstrate its ease of use by teaching it to 3 elementary school boys in less than an hour.
   Officer: That may be, but I think diplomats would have a hard time with it.
   P: That is a problem with the diplomats, not with the cipher.

The Playfair Cipher: Use

1. Was probably used in the Boer Wars (1880-1902).

The Playfair Cipher: Use

1. Was probably used in the Boer Wars (1880-1902).
2. Was used in WW II in the Pacific by the Americans. Was used to rescue JFK when the PT 109 sank.

The Rail Fence Cipher

September 27, 2020

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

In current case of 3 rows and message of length 11 we did

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

In current case of 3 rows and message of length 11 we did

First list out the letters in positions $\equiv 1 \pmod 4$.

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

In current case of 3 rows and message of length 11 we did

First list out the letters in positions $\equiv 1 \pmod 4$.

Second list out the letters in positions $\equiv 0, 2 \pmod 4$.

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

In current case of 3 rows and message of length 11 we did

First list out the letters in positions $\equiv 1 \pmod 4$.

Second list out the letters in positions $\equiv 0, 2 \pmod 4$.

Third list out letters in positions $\equiv 3 \pmod 4$).

Rail Fence Cipher as Understood In Past

Key is 3. Message is **Marina is a TA** .

Write it in three rows as such:

M N A

A I A S T

R I A

Write each row: **MNAAIASTRIA**

How would you describe this cipher in modern terminology?

Discuss

In current case of 3 rows and message of length 11 we did

First list out the letters in positions $\equiv 1 \pmod 4$.

Second list out the letters in positions $\equiv 0, 2 \pmod 4$.

Third list out letters in positions $\equiv 3 \pmod 4$)).

Leave as an exercise what happens if k rows, n letter message.

The Rail Fence Cipher History

The Rail Fence Cipher History

1. Used in Ancient time.

The Rail Fence Cipher History

1. Used in Ancient time.
2. Could have been combined with Shift.

The Rail Fence Cipher History

1. Used in Ancient time.
2. Could have been combined with Shift.
3. Pretty good if Eve does not know you are using it, so good if you do not believe Kerckhoff's Principle.

The Rail Fence Cipher History

1. Used in Ancient time.
2. Could have been combined with Shift.
3. Pretty good if Eve does not know you are using it, so good if you do not believe Kerckhoff's Principle.
4. We do believe Kerckhoff's Principle.

The Autokey Cipher

September 27, 2020

The AutoKey Cipher: A Variant of Vig

IDEA: Use the plaintext as a Key after a start.

The AutoKey Cipher: A Variant of Vig

IDEA: Use the plaintext as a Key after a start.

1. There is a key, a short word or phrase. We'll use **Metz** .
2. **Metz** is $(12, 4, 19, 25)$. We shift the first letter by 12, the second by 4, the third by 19, he fourth by 25.
3. After first four use plaintext lagged by 4.

The AutoKey Cipher: A Variant of Vig

IDEA: Use the plaintext as a Key after a start.

1. There is a key, a short word or phrase. We'll use **Metz** .
2. **Metz** is $(12, 4, 19, 25)$. We shift the first letter by 12, the second by 4, the third by 19, he fourth by 25.
3. After first four use plaintext lagged by 4.

Example Key is **Metz** and I want to encode **Joe Biden is running.** So Key is metzjoebidenisrunning

The AutoKey Cipher: A Variant of Vig

IDEA: Use the plaintext as a Key after a start.

1. There is a key, a short word or phrase. We'll use **Metz** .
2. **Metz** is $(12, 4, 19, 25)$. We shift the first letter by 12, the second by 4, the third by 19, he fourth by 25.
3. After first four use plaintext lagged by 4.

Example Key is **Metz** and I want to encode **Joe Biden is running.** So Key is metzjoebidenisrunning

1. Encode (j,o,e,b) by shifting by $(12, 4, 19, 25)$.

The AutoKey Cipher: A Variant of Vig

IDEA: Use the plaintext as a Key after a start.

1. There is a key, a short word or phrase. We'll use **Metz** .
2. **Metz** is $(12, 4, 19, 25)$. We shift the first letter by 12, the second by 4, the third by 19, he fourth by 25.
3. After first four use plaintext lagged by 4.

Example Key is **Metz** and I want to encode **Joe Biden is running.** So Key is metzjoebidenisrunning

1. Encode (j,o,e,b) by shifting by $(12, 4, 19, 25)$.
2. Encode

$$(i, d, e, n, i, s, r, u, n, n, i, n, g)$$

by the shift induced by

$$(j, o, e, b, i, d, e, n, i, s, r, u, n)$$

To Decode will need to do this four letters at a time.

AutoKey Pros and Cons

PROS: The techniques for cracking Vig do not work.
PROS: If Eve does not know you are using it, seems uncrackable.

CON: Complicated to use (more on that next slide).

Question: How would you crack it?

AutoKey Pros and Cons

PROS: The techniques for cracking Vig do not work.
PROS: If Eve does not know you are using it, seems uncrackable.

CON: Complicated to use (more on that next slide).

Question: How would you crack it?

Similar to Book Cipher in that the key and the message are **both** in English so can use freq somewhat.

If guess the key word then rest is EASY!

Autokey History

1. Invented in 1586 by Blaise de Vigenere.

Autokey History

1. Invented in 1586 by Blaise de Vigenere.
2. People found it hard to use so they simplified it into what we now call the Vig cipher.

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right?

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".

Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good.

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good. Reminds me of a quote:

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good. Reminds me of a quote: During one of the baseball strikes the major league owners were threatening to replace the players with people of far worse quality who were not in the major or minor leagues.

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good. Reminds me of a quote: During one of the baseball strikes the major league owners were threatening to replace the players with people of far worse quality who were not in the major or minor leagues. Comedian Bill Mahr observed:
   If the hitters suck, and the pitchers suck, who's going to know?

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good. Reminds me of a quote: During one of the baseball strikes the major league owners were threatening to replace the players with people of far worse quality who were not in the major or minor leagues. Comedian Bill Mahr observed:
   If the hitters suck, and the pitchers suck, who's going to know?

That could be why Playfair was not cracked!

Marina's Opinion (TA-2019)

I just think its a little weird how unmathematical some of these ciphers are, like Playfair and Rail Fence. It seems like the kind of thing a child might have come up with and I don't see the mathematical intuition behind it. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".
Is she right? Mostly yes:

1. **Yes.** Before 1900 cryptography was not a mathematical study.
2. **Caveat.** Crackers also not very good. Reminds me of a quote: During one of the baseball strikes the major league owners were threatening to replace the players with people of far worse quality who were not in the major or minor leagues. Comedian Bill Mahr observed:
   If the hitters suck, and the pitchers suck, who's going to know?

That could be why Playfair was not cracked! Unless it was.

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

Def Book Cipher:

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

Def Book Cipher:

1. Alice and Bob agree on a book to be the key.

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

Def Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a mesage Alice specifies, for each word,
   - A page number. E.g., Page 19.
   - A line number. E.g., Line 24 (On Page 19).
   - A word number. E.g., Word 4 (On Page 19, Line 24).

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

Def Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a mesage Alice specifies, for each word,
   - A page number. E.g., Page 19.
   - A line number. E.g., Line 24 (On Page 19).
   - A word number. E.g., Word 4 (On Page 19, Line 24).
3. Alice will try to use differeng triples for the same word.

(Another) Book Cipher

The term **Book Cipher** was used both for the Vig cipher where key is a book and for what I will discuss now.

Def Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a mesage Alice specifies, for each word,
   - A page number. E.g., Page 19.
   - A line number. E.g., Line 24 (On Page 19).
   - A word number. E.g., Word 4 (On Page 19, Line 24).
3. Alice will try to use differeng triples for the same word.
4. Bob has same book so can decode.

Security Known to be crackable, but won't go into that here.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!