

# BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

# PIN Numbers

# 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 premiered 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 premiered in 2018.

Eve is tracking an assassin 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 premiered in 2018.

Eve is tracking an assassin 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 premiered in 2018.

Eve is tracking an assassin 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 premiered in 2018.

Eve is tracking an assassin 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

# The Autokey Cipher

# 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** .

# 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.



# 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, the 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, the 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, the 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

*(j, o, e, b, 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.



# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

**Def** Book Cipher:

# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

**Def** Book Cipher:

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

# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

**Def** Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a message 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).

# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

**Def** Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a message 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 different triples for the same word.

# Book Cipher

(Not to be confused with Vig-Book-Cipher.)

**Def** Book Cipher:

1. Alice and Bob agree on a book to be the key.
2. To send a message 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 different 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!!!