MISC STUFF

September 6, 2019

If you DID NOT get an email

If you DID NOT get an email last night at around 8:30PM then let me know- it means you are not on the list.

If you ADDED the course recently you might be in that category.

Rules on HW

1. HW submitted on Gradescope.
2. Must be electronically submitted (no scanned hand-written documents).
3. When HW is posted we will also supply latex and plaintext of the HW to make it easier for you.

Office Hours

1. Bill G Office Hours MW 1:00-1:45 and 3:30-5:00 in IRB 2242.
2. Office Hours for TAs will be in IRB study area 3232. (NOTE-3232 is a terrible pin number, though not in the top 20. See next slide.)
3. Times listed under policy on course website. We cover most of Monday, Tuesday, Wedensday between 11 and 5, except class time.

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? Raise hands.

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? Raise hands.

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? Raise hands.

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?

Shift Cipher Numbers

I had said that if q_i is prob of letter i then

1. $\sum_{i=0}^{25} q_i q_i \sim 0.065$
2. If $s \ne 0$ $\sum_{i=0}^{25} q_i q_{i+s \pmod{26}} \le\sim 0.038$
3. NOTE- there is a big gap.

Justin actually DID this (as part of hw 01) and found

1. $\sum_{i=0}^{25} q_i q_i \sim 0.065$
2. If $s \ne 0$ $\sum_{i=0}^{25} q_i q_{i+s \pmod{26}} \sim 0.049$
3. NOTE- there is still big gap.
4. I have corrected the slide.

Where did prior number come from and why was it wrong? Freq changed over time and Bill had an old one? Bill copied it wrong? The world may never know! But its been fixed now. Yeah Justin!

Making Vig Harder to Crack

Usual Vig

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

encrypts to

MOIRP VUWTC WYDDN BOFGS DXUU

Getting More Out of Your Phrase

If the key was

Corn Flake

You would get a key of length 9. We want More

Getting More Out of Your Phrase

If the key was

Corn Flake

You would get a key of length 9. We want More

Corn is 4 letters long. Flake is 5 letters long
We form a key of length $LCM(4,5) = 20$. (Won't fit on line! Oh Well.)

C	O	R	N	C	O	R	N	C	O	R	N	C	O	R	N	C
F	L	A	K	E	F	L	A	K	E	F	L	A	K	E	F	L
7	25	17	23	6	19	2	13	12	18	22	24	2	24	21	18	1

ADD it up to get new 20-long key.

If phrase is Wheel of Fortune and you did the above trick, how long a key do you get? Discuss

Getting More Out of Your Phrase

If the key was

Corn Flake

You would get a key of length 9. We want More

Corn is 4 letters long. Flake is 5 letters long
We form a key of length $LCM(4, 5) = 20$. (Won't fit on line! Oh Well.)

C	O	R	N	C	O	R	N	C	O	R	N	C	O	R	N	C
F	L	A	K	E	F	L	A	K	E	F	L	A	K	E	F	L
7	25	17	23	6	19	2	13	12	18	22	24	2	24	21	18	1

ADD it up to get new 20-long key.

If phrase is Wheel of Fortune and you did the above trick, how long a key do you get? Discuss $LCM(5, 2, 7) = 70$.

Can Eve Still Crack Vig?

Can Eve Still Crack Vig?

Can Eve Still Crack Vig?

Can Eve Still Crack Vig?
Yes (in the modern era) but its harder because of longer key.
This is Important: The first goal is to make a encryption system that is hard to crack. If not possible then make one that is harder to crack.

Change Key's but how often? If crackable but takes time then can change key's on a regular basis so just when they crack it, BOOM- you've changed key's!

In an older era this may have made Vig go from crackable to uncrackable.

Book Cipher

Book Cipher

A student said

Lets use Vig cipher with a book for the key

Is it a good idea? Discuss

Book Cipher

A student said

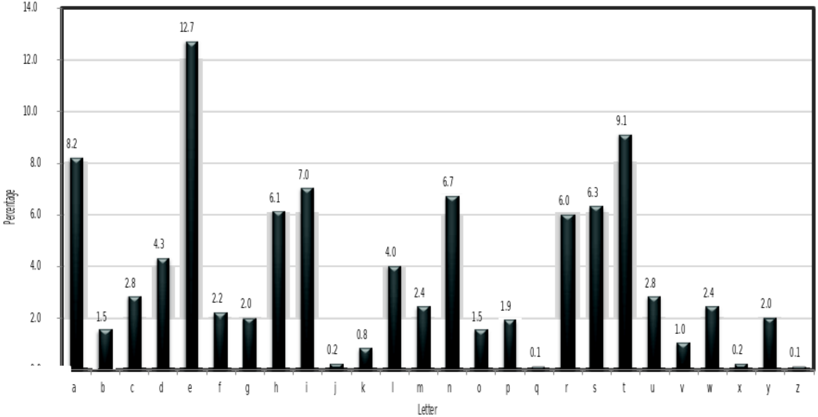
Lets use Vig cipher with a book for the key

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.

1. (z, e): Hmm, z is unlikely but e is likely.
2. (a, d): Hmm, seems more likely than (z, e).
3. Can rank which are more likely (e.g., add the freqs).
4. Can then use adjacent letters and freq of adjacent pairs, and rank them.
5. Triples. Etc.

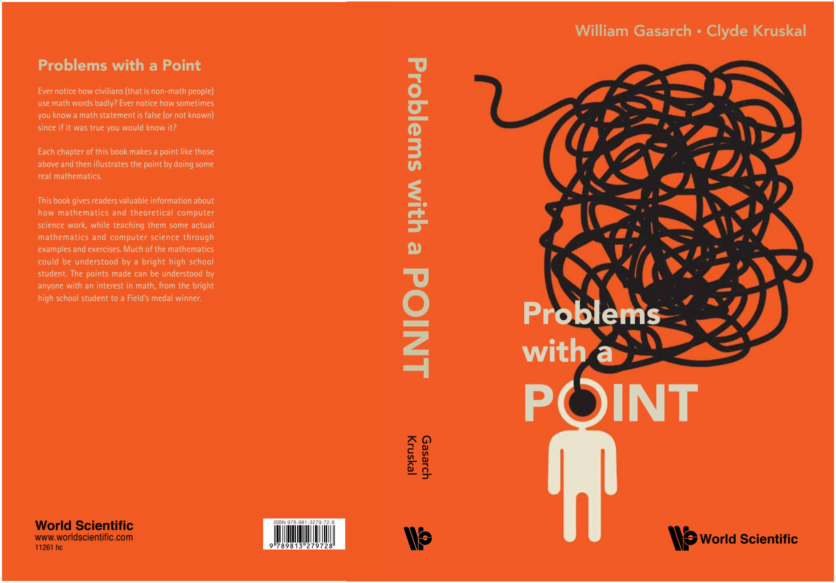
Book Cipher was Really Used

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

Were these good choices? NO. They are books one 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

Vig Cipher with Key Longer Than Message

The 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 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.

Gen 2-letter Sub and Matrix Codes

Shift, Affine, Vig, Gen Sub, Easy to Crack

Shift, Affine, Vig all 1-letter substitutions. Freq cracked them.
Idea: Lets substitute two letters at a time.
An Idea Which History Passed By:
Definition: Gen Sub 2-Cipher with perm f on $\{0, \ldots, 25\}^2$.

1. Encrypt via $xy \rightarrow f(xy)$.
2. Decrypt via $xy \rightarrow f^{-1}(xy)$

Why never used?

1. It was used but they kept it hidden and still not known!
2. The key length is roughly $26^2 \times 10 = 6760$ bits.
3. Past: hard to use. Present: Crackable with freq of pairs.

Need bijection of $\{0, \ldots, 25\} \times \{0, \ldots, 25\}$ that is easy to use.

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \rightarrow M(xy)$.
2. Decrypt via $xy \rightarrow M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
HEY- WAIT A MINUTE!

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
HEY- WAIT A MINUTE!
Easy to see if M^{-1} exists? Easy to find M^{-1}?

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \rightarrow M(xy)$.
2. Decrypt via $xy \rightarrow M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
HEY- WAIT A MINUTE!
Easy to see if M^{-1} exists? Easy to find M^{-1}?
Is Bill punking you . . . again?

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \rightarrow M(xy)$.
2. Decrypt via $xy \rightarrow M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
HEY- WAIT A MINUTE!
Easy to see if M^{-1} exists? Easy to find M^{-1}?
Is Bill punking you ... again? No he is not.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$M^{-1} = \frac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Do you recognize the expression $ad - bc$?

The Matrix Cipher

Definition: Matrix Cipher. Pick M a 2×2 matrix.

1. Encrypt via $xy \rightarrow M(xy)$.
2. Decrypt via $xy \rightarrow M^{-1}(xy)$

Encode: Break T into blocks of 2, apply M to each pair.

Decode: Do the same only with M^{-1}.
HEY- WAIT A MINUTE!
Easy to see if M^{-1} exists? Easy to find M^{-1}?
Is Bill punking you ... again? No he is not.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then

$$M^{-1} = \frac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Do you recognize the expression $ad - bc$? Determinant!

Inverse Matrix in $\mathbb{C}$ and in Mods

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

1. Matrix M over $\mathbb{C}$ has an inverse iff $ad - bc \neq 0$.
2. Matrix M over Mod n has an inverse iff $ad - bc$ has an inverse mod n. This is equiv to $ad - bc$ being rel prime to n.
3. Matrix M over Mod 26 has an inverse iff $ad - bc$ is rel prime to 26. This is equiv to $ad - bc$ is not div by 2 or 13.

Stuff to know about matrices:

1. A matrix is invertible iff all of the rows are linearly ind.
2. If over $\mathbb{Z}_p$ where p is a prime then more like $\mathbb{C}$: all numbers have inverses so need $ad - bc \not\equiv 0 \pmod{p}$.

The Matrix Cipher

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Good News:

1. Can test if M^{-1} exists, and if so find it easily.
2. M small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.

Bad News:

1. Eve CAN crack using frequencies of pairs of letters.
2. Eve CAN crack by brute force since Key Space is $\sim 26^4 = 456976$.

So what to do?

The Matrix Cipher

Definition: Matrix Cipher. Pick n and M an $n \times n$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \to M(\vec{x})$.
2. Decrypt via $\vec{y} \to M^{-1}(\vec{y})$

We'll take $n = 9$.

The Matrix Cipher

Definition: Matrix Cipher. Pick n and M an $n \times n$ matrix with det rel prime to 26.

1. Encrypt via $\vec{x} \rightarrow M(\vec{x})$.
2. Decrypt via $\vec{y} \rightarrow M^{-1}(\vec{y})$

We'll take $n = 9$.

1. Can determine if M has inv and if so find it easily.
2. M still small, so Key small.
3. Applying M or M^{-1} to a vector is easy computationally.
4. Eve can crack using freqs of 9-long sets of letters? Hard?
5. Eve cannot use brute force – Key Space is $\sim 26^{81}$ (next slide shows how one could try this).

Can crack in $O(26^{n^2})$

1. Input C, a coded text. Know n.
2. For EVERY $n \times n$ invertible matrix A over $\mathbb{Z}_{26}$,
    2.1 Decode C into m using A.
    2.2 IF LOOKS-LIKE-ENGLISH(m)=YES then STOP and output m. else goto next matrix A

Takes roughly $O(26^{n^2})$ steps.
Can we do better? VOTE.

1. YES
2. NO - and we can PROVE we can't do better with ciphertext-only.
3. UNKNOWN TO SCIENCE if we can do better with ciphertext-only.

Can crack in $O(26^{n^2})$

1. Input C, a coded text. Know n.
2. For EVERY $n \times n$ invertible matrix A over $\mathbb{Z}_{26}$,
    - 2.1 Decode C into m using A.
    - 2.2 IF LOOKS-LIKE-ENGLISH(m)=YES then STOP and output m. else goto next matrix A

Takes roughly $O(26^{n^2})$ steps.
Can we do better? VOTE.

1. YES
2. NO - and we can PROVE we can't do better with ciphertext-only.
3. UNKNOWN TO SCIENCE if we can do better with ciphertext-only.

YES- we can do $O(n26^n)$.

Can crack in $O(n26^n)$

The attack in the last slide went through every Matrix.
Better Idea: We take life one row at a time.
Example: 3×3 matrix cipher. Decode Matrix B.

$$C = c_1 c_2 \cdots c_N \text{ each } c_i \text{ is 3-long}$$

Guess the first row of B. Say:

$$\begin{pmatrix} 1 & 1 & 7 \\ * & * & * \\ * & * & * \end{pmatrix}$$

Let $Bc_i = m_i$. Then $(1,1,7) \cdot t_i = m_i^1$ is first letter of m_i.

$$(m_1^1, m_2^1, m_3^1, \ldots, m_N^1)$$

is every third letter. Can do IS-ENGLISH on it.

Can crack in $O(n26^n)$

Eve knows that Alice and Bob decode with $n \times n$ Matrix B. Ciphertext is

$$C = c_1 c_2 \cdots c_N \qquad c_i = c_i^1 \cdots c_i^n$$

```
For $i = 1$ to $n$
    For all $r \in \mathbb{Z}_{26}^n$ (guess that $r$ is $i$th row of $B$).
        $T = (r \cdot c_1, \ldots, r \cdot c_N)$ (Is every $i$th letter.)
        IF IS-ENGLISH($T$)=YES then $r_i = r$ and goto next $i$. Else
        goto the next $r$.
```

B is

$$\begin{pmatrix} \cdots & r_1 & \cdots \\ \vdots & \vdots & \vdots \\ \cdots & r_n & \cdots \end{pmatrix}$$

Takes roughly $O(n26^n)$ steps.

Important Lesson

Assume: 26^{80} time is big enough to thwart Eve.

1. If we think that best Eve can do is $O(26^{n^2})$ then we take $n = 9$, so Eve needs $O(26^{81})$.
2. If we think that best Eve can do is $O(n26^n)$ then we take $n = 80$, so Eve needs $O(80 \times 26^{80})$.

The $O(n \times 26^n)$ cracking does not show that Matrix Cipher is insecure, but it still is very important: Alice and Bob must increase their parameters. That is already a win since it makes life harder for Alice and Bob.

The History of Cryptography in One Slide

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).
2. Alice and Bob think its uncrackable and have a “proof” that it is uncrackable (e.g., Eve HAS to go through all 26^{81} matrices).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{81} matrices).
3. Eve Cracks it. (The trick above- only about 9×26^{9}.)

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).
2. Alice and Bob think its uncrackable and have a “proof” that it is uncrackable (e.g., Eve HAS to go through all 26^{81} matrices).
3. Eve Cracks it. (The trick above- only about 9×26^9.)
4. Lather, Rinse, Repeat.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).
2. Alice and Bob think its uncrackable and have a “proof” that it is uncrackable (e.g., Eve HAS to go through all 26^{81} matrices).
3. Eve Cracks it. (The trick above- only about 9×26^{9}.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 9$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{81} matrices).
3. Eve Cracks it. (The trick above- only about 9×26^9.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

Proofs rely on limiting what Eve can do, and hence do not work if Eve does something else.

Why is Matrix Cipher Not Used?

Matrix Cipher with $n \times n$ Matrices.
The best known attack is $O(n26^n)$. So why isn't it used? Discuss

Why is Matrix Cipher Not Used?

Matrix Cipher with $n \times n$ Matrices.
The best known attack is $O(n26^n)$. So why isn't it used? Discuss
Types of attacks:

1. Ciphertext Only. That is what we are studying: Eve just gets send text T.
2. Plaintext-Ciphertext Pairs. In reality Eve has prior messages and what they coded to.

If Eve has yesterdays texts and what they decoded to, can help her today. (Next Slide.) That is why not used.

Cracking Matrix Cipher

Example using 2 × 2 Matrix Cipher.
Eve learns that (19,8) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 19a + 8b &= 3 \\ 19c + 8d &= 9 \end{aligned}$$

Two linear equations, Four variables

Cracking Matrix Cipher

Example using 2 × 2 Matrix Cipher.
Eve learns that (19,8) encrypts to $(3, 9)$. Hence:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

So

$$\begin{aligned} 19a + 8b &= 3 \\ 19c + 8d &= 9 \end{aligned}$$

Two linear equations, Four variables

If Eve learns one more 2-letter message decoding then she will have

Four linear equations, Four variables

which she can solve! Yeah? Boo? Depends whose side you are on.

The One-Time Pad

One-time pad

- Let $\mathcal{M} = \{0,1\}^n$, the set of all messages.
- *Gen*: choose a uniform key $k \in \{0,1\}^n$
- $Enc_k(m) = k \oplus m$
- $Dec_k(c) = k \oplus c$
- Correctness:

$$\begin{aligned} Dec_k(Enc_k(m)) &= k \oplus (k \oplus m) \\ &= (k \oplus k) \oplus m \\ &= m \end{aligned}$$

Example Of One-time pad

Key is 100010100010001111101111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Example Of One-time pad

Key is 10001010001000111110111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:
VOTE: Yes, No, or Other.

Example Of One-time pad

Key is 100010100010001111101111100

Alice wants to send Bob 1110.

She sends $1110 \oplus 1000 = 0110$

Then Bob wants to send Alice 00111.

He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:

VOTE: Yes, No, or Other.

Yes. Really!

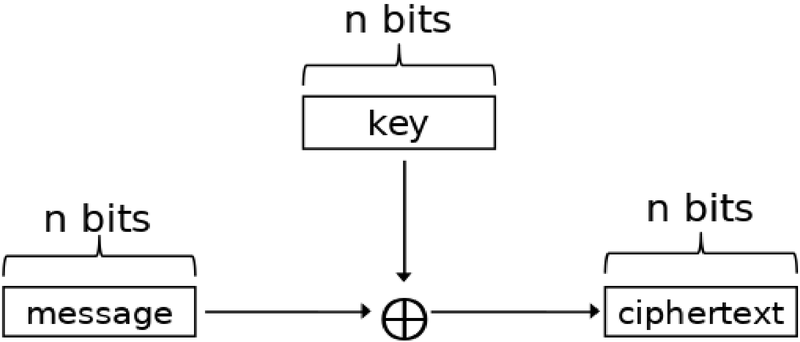
Example Of One-time pad

Key is 1000101000100011111011111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:
VOTE: Yes, No, or Other.
Yes. Really!
Caveat: Generating truly random bits is hard.

One-time pad



One-time pad

- Patented in 1917 by Vernam
- Historical research indicates it was invented (at least) 35 years earlier
- Proven perfectly secret by Shannon (1949)

Linear Congruential Generators Can Be Broken

NOTE ABOUT THE SLIDES

This section on Random Bits Are Hard I did just the beginning on Wed Sept 4, and did it from the beginining on Mo Sept 9. Even so, I present the whole thing in both these slides and the next slide packet.

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018
Student: You said that generating Random Bits is hard. Why?

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018
Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018
Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018

Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

Bill: Okay. How do they do it, and is it *Truly* Random?

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018

Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

Bill: Okay. How do they do it, and is it *Truly* Random?

Student: Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018
Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

Bill: Okay. How do they do it, and is it *Truly* Random?

Student: Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!
[That last line is fictional.]

How Hard is it to Generate Truly Random Bits?

Paraphrase of a Piazza conversation from Fall 2018
Student: You said that generating Random Bits is hard. Why?

Bill: *Truly* Rand Bits are hard. How would you do it?

Student: Just use the Random function in Java!

Bill: Okay. How do they do it, and is it *Truly* Random?

Student: Enlighten me as to how Java does it and why it does not work. You are truly the wisest of them all!
[That last line is fictional.]

Bill: I will show what Java does and why it bytes.

How does Java Produce Random Numbers

Java (and most languages) use a Linear Congruential Generator. When the computer is turned on (and once a month after that):

1. m is a large power of two, close to capacity.
2. a, c, r_0 are random-looking. E.g. the number of nanoseconds mod m since last time reboot.
3. The computer has the recurrence

$$r_{i+1} = a * r_i + c \pmod{m}$$

4. The ith time a random number is chosen, use r_i.
5. Computer need only keep r_i, a, c, m in memory.

Depending on a, c, r_0 this can look random... or not.

We look at a Random Looking Recurrence

$x_0 = 2134,\ A = 4381,\ B = 7364,\ M = 8397.$

$$\begin{aligned} x_0 &= 2134 \text{ view as } 21, 34 \\ x_{n+1} &= 4381x_n + 7364 \pmod{8397} \end{aligned}$$

We use this to generate random-looking bits, and use in Cipher.

We will then crack it.

Awesome Vig or Psuedo One Time Pad

$A = 01$, $B = 02$, $\cdots$ $Z = 26$ (Not our usual since $A = 01$.)
View each letter as a two-digit number mod 26.
Want a LONG sequence of 2-digit numbers $k_1, k_2, \ldots$

1. Will code $m_1, m_2, \ldots$ by, for each digit adding mod 10.
   Example: If key is 12 38 and message is 29 23 then send

   $$\begin{array}{cc} 12 & 38 \\ 29 & 23 \\ \hline 31 & 51 \end{array}$$

   So send 31 51 (these do not correspond to letters, thats fine).

   $$(m_1 + k_1 \pmod{10}, m_2 + k_2 \pmod{10}, \ldots$$

2. Can view as either a Vig with a very long key OR as a 1-time pad. We view as Vig since not truly 1-time pad.

How to get a long random (looking?) sequence? Next slide.

Use Rec. x_0, A, B, M is Short Private Key

(Example from *"Cracking" a Random Number Generator by James Reed.* Paper on Course Website.)

$x_0 = 2134$, $A = 4381$, $B = 7364$, $M = 8397$.

$$\begin{aligned} x_0 &= 2134 \text{ view as } 21, 34 \\ x_{n+1} &= 4381x_n + 7364 \pmod{8397} \end{aligned}$$

We show that this random-looking sequence is NOT that random and, if used for a psuedo-one-time-pad, can be cracked.

Example

$x_0 = 2134$
$x_1 = 2160$
$x_2 = 6905$
$x_3 = 3778$
They start with x_1.
If the document began with the word secret then encode:

Text-Letter	S	E	C	R	E	T
Text-Digits	19	05	03	18	05	20
Key–Digits	21	60	69	05	37	78
Ciphertext	30	65	62	13	32	98

Example

Alice sends Bob a document using the x_i as a Vig coding two chars at a time.

Eve knows rec of form $x_{n+1} = Ax_n + B \pmod{M}$.

Eve knows that A, B, M are all 4-digits.

Example

Alice sends Bob a document using the x_i as a Vig coding two chars at a time.

Eve knows rec of form $x_{n+1} = Ax_n + B \pmod{M}$.

Eve knows that A, B, M are all 4-digits.

Eve knows that the document is about India and Pakistan.

Eve thinks Pakistan will be in the document.

Text-Letter	P	A	K	I	S	T	A	N
Text-Digits	16	01	11	09	19	20	01	14

Eve can crack it!

Eve tries PAKISTAN on every sequence of 8 letters. We describe what tries means.

Text-Letter	P	A	K	I	S	T	A	N
Text-Digits	16	01	11	09	19	20	01	14
Ciphertext	24	66	87	47	17	45	26	96

If Eve's guess is correct then:

Key–Digits	18	65	76	48	08	25	25	82

Since $x_{n+1} = Ax_n + B \pmod{M}$

$7648 \equiv 1865A + B \pmod{M}$

$825 \equiv 7648A + B \pmod{M}$

$2582 \equiv 825A + B \pmod{M}$

Can we solve these? (The title Eve can crack it! gives it away!)

Eve can crack it!

EQ1: $7648 \equiv 1865A + B \pmod{M}$
EQ2: $825 \equiv 7648A + B \pmod{M}$
EQ3: $2582 \equiv 825A + B \pmod{M}$

By looking at EQ2$-$EQ1 and EQ3$-$EQ1 get 2 equations and no B
EQ4: $-6823 \equiv 5783A \pmod{M}$
EQ5: $-5066 \equiv -1040A \pmod{M}$

Mult EQ4 by 5066 and EQ5 by 6823 and subtract to get

$$-36,392,598 \equiv 0 \pmod{M}$$

Can we use this?

Eve can crack it!

EQ1: $7648 \equiv 1865A + B \pmod{M}$
EQ2: $825 \equiv 7648A + B \pmod{M}$
EQ3: $2582 \equiv 825A + B \pmod{M}$

By looking at EQ2$-$EQ1 and EQ3$-$EQ1 get 2 equations and no B
EQ4: $-6823 \equiv 5783A \pmod{M}$
EQ5: $-5066 \equiv -1040A \pmod{M}$

Mult EQ4 by 5066 and EQ5 by 6823 and subtract to get

$$-36,392,598 \equiv 0 \pmod{M}$$

Can we use this? Do chickens have lips!

Eve can crack it!

$$36,392,598 \equiv 0 \pmod{M}$$

M divides $36,392,598$.
Hence a SMALL number of possibilities for M.
Eve factors 36,392,598.

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$

Eve can crack it!

$$36,392,598 \equiv 0 \pmod{M}$$

M divides $36,392,598$.
Hence a SMALL number of possibilities for M.
Eve factors 36,392,598.

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?

Eve can crack it!

$$36,392,598 \equiv 0 \pmod{M}$$

M divides $36,392,598$.
Hence a SMALL number of possibilities for M.
Eve factors 36,392,598.

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?

Eve can crack it!

$$36,392,598 \equiv 0 \pmod{M}$$

M divides $36,392,598$.
Hence a SMALL number of possibilities for M.
Eve factors 36,392,598.

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
Will come back to this.

Eve can crack it!

$$36,392,598 \equiv 0 \pmod{M}$$

M divides $36,392,598$.
Hence a SMALL number of possibilities for M.
Eve factors 36,392,598.

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
Will come back to this.

1. M is a divisor of $36,392,598$
2. M is 4 digits long
3. The cipher used 7648, so $M > 7648$

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \leq M \leq 9999$.

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598$

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598$
6. If use 311 and 27: $311 \times 27 = 8397$. WORKS!

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \leq M \leq 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598$
6. If use 311 and 27: $311 \times 27 = 8397$. WORKS!
7. Leave it to you to show that using 197 does not work.

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598$
6. If use 311 and 27: $311 \times 27 = 8397$. WORKS!
7. Leave it to you to show that using 197 does not work.
8. So $M = 8397$.

Eve Can Crack It!—Almost There

$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of $36,392,598$ such that $7648 \le M \le 9999$.

1. Can't use 197 AND 311 since $197 \times 311 \sim 200 \times 300 = 60000$
2. If use 311 then need at least one 3: $2 \times 11 \times 311 = 6842$
3. If use 311 and exactly one 3 does not work: (a) $311 \times 3 \times 2 = 1866$ (b) $311 \times 3 \times 11 = 10263$.
4. If use 311 and ≥ 2 3's then no 11: $311 \times 11 \times 9 = 30789$
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598$
6. If use 311 and 27: $311 \times 27 = 8397$. WORKS!
7. Leave it to you to show that using 197 does not work.
8. So $M = 8397$.

Eve Can Crack It!

EQ4: $-6823 \equiv 5783A \pmod{M}$
EQ5: $-5066 \equiv -1040A \pmod{M}$
$M = 8397$

EQ4: $-6823 \equiv 5783A \pmod{8397}$
EQ5: $-5066 \equiv -1040A \pmod{8397}$
5783 has an inverse mod 8397 so can find A from EQ4.

Find $A = 4381$

EQ1: $7648 \equiv 1865A + B \pmod{M}$
Use to find $B = 7364$.

If no solution then PAKISTAN was not there, try next spot.

Not done yet: use this to decode and see if it looks like English.

Eve Can Factor Fast?

Eve had to factor:

$$36,392,598 = 2 \times 3^3 \times 11 \times 197 \times 311$$

We usually say

Factoring is Hard

Lets be careful there.

1. If ALICE picks two primes p, q of length n and picks $N = pq$ then factoring N is hard.
2. If a RANDOM number is given then half the time its even. A third of the time is divided by 3. Not so hard to factor.

Our scenario is closer to RANDOM than to ALICE.