Linear Congruential Generators Can Be Broken

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 does Java do it? 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 does Java do it? 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 does Java do it? 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 does Java do it? 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. If make it a power of 2, easier for Alice and Bob, but also for Eve.
2. A, B, r_0 are random-looking. E.g. the number of nanoseconds mod M since last time reboot.
3. The computer has the recurrence

$$r_{i+1} = A \times r_i + B \pmod{M}$$

4. The ith time a random number is chosen, use r_i.
5. Computer need only keep r_i, A, B, 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 Vig-type Cipher.

We will then crack it.

We will assume we know that the random numbers ae generated by a recurrence of the form

$$r_{i+1} = A \times r_i + B \pmod{M}$$

but that we do not know r_0, A, B, M.

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 which is not what we usually do!!!!!!!!!!!
   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. View as (1) Vig with long key OR (2) psuedo One-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.)

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

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

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. If she fails she may try again with 6-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. If she fails she may try again with 6-digits.

Eve knows that the document is about India and Pakistan.

Eve thinks Pakistan will be in the document.
Eve thinks M is 4-digits.

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!

$$\begin{aligned}
\text{EQ1: } & 7648 \equiv 1865A + B \pmod{M} \\
\text{EQ2: } & 825 \equiv 7648A + B \pmod{M} \\
\text{EQ3: } & 2582 \equiv 825A + B \pmod{M}
\end{aligned}$$

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

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: $-5066 \equiv -1040A \pmod{M}$

Eve can crack it! (cont)

EQ4: $-6823 \equiv 5783A \pmod{M}$

EQ5: $-5066 \equiv -1040A \pmod{M}$

Eve can crack it! (cont)

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

Mult EQ4 by 1040 and EQ5 by 5783 to get:

EQ4': $-6823 \times 1040 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-5066 \times 5783 \equiv -1040 \times 5783 \times A \pmod{M}$

Eve can crack it! (cont)

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

Mult EQ4 by 1040 and EQ5 by 5783 to get:

EQ4': $-6823 \times 1040 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-5066 \times 5783 \equiv -1040 \times 5783 \times A \pmod{M}$

We rewrite a bit:

Eve can crack it! (cont)

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

Mult EQ4 by 1040 and EQ5 by 5783 to get:

EQ4': $-6823 \times 1040 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-5066 \times 5783 \equiv -1040 \times 5783 \times A \pmod{M}$

We rewrite a bit:

EQ4': $-7095920 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-29296678 \equiv -5783 \times 1040 \times A \pmod{M}$

Eve can crack it! (cont)

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

Mult EQ4 by 1040 and EQ5 by 5783 to get:

EQ4': $-6823 \times 1040 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-5066 \times 5783 \equiv -1040 \times 5783 \times A \pmod{M}$

We rewrite a bit:

EQ4': $-7095920 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-29296678 \equiv -5783 \times 1040 \times A \pmod{M}$

Add EQ4' and EQ5' to get: $-36392598 \equiv 0 \pmod{M}$
Can we use this?

Eve can crack it! (cont)

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

Mult EQ4 by 1040 and EQ5 by 5783 to get:

EQ4': $-6823 \times 1040 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-5066 \times 5783 \equiv -1040 \times 5783 \times A \pmod{M}$

We rewrite a bit:

EQ4': $-7095920 \equiv \quad 5783 \times 1040 \times A \pmod{M}$
EQ5': $-29296678 \equiv -5783 \times 1040 \times A \pmod{M}$

Add EQ4' and EQ5' to get: $-36392598 \equiv 0 \pmod{M}$
Can we use this? Yes We Can!

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$$

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
We will address this point later.

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
We will address this point later.

1. M is a divisor of 36392598

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
We will address this point later.

1. M is a divisor of 36392598
2. M is 4 digits long

Eve can crack it!

$$36392598 \equiv 0 \pmod{M}$$

M divides 36392598.
Hence a SMALL number of possibilities for M.
Eve factors 36392598.

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
Factoring? Really? Eve has to Factor?
(Sarcastic) does she have a quantum computer?
We will address this point later.

1. M is a divisor of 36392598
2. M is 4 digits long
3. The cipher used 7648, so $M > 7648$

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have?

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$

M is a factor of 36392598 such that $7648 < M \leq 9999$.

How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.
4. If use 311, at least two 3's, and 11:
   $311 \times 11 \times 9 = 30789 > 9999$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.
4. If use 311, at least two 3's, and 11:
   $311 \times 11 \times 9 = 30789 > 9999$.
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598 < 7648$.

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.
4. If use 311, at least two 3's, and 11:
   $311 \times 11 \times 9 = 30789 > 9999$.
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598 < 7648$.
6. If use 311 and 27: $311 \times 27 = 8397$. WORKS!

Eve Can Crack It!—Almost There

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.
4. If use 311, at least two 3's, and 11:
   $311 \times 11 \times 9 = 30789 > 9999$.
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598 < 7648$.
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

$36392598 = 2 \times 3^3 \times 11 \times 197 \times 311$
M is a factor of 36392598 such that $7648 < M \leq 9999$.
How many factors does $2 \times 3^3 \times 11 \times 197$ have? $2 \times 4 \times 2 \times 2 = 32$.

1. Can't use 197 AND 311: $197 \times 311 = 61267 > 9999$.
2. If use 311 then need a 3: $2 \times 11 \times 311 = 6842 < 7648$.
3. If use 311 and exactly one 3 does not work:
   (a) Use 2 but not 11: $311 \times 3 \times 2 = 1866 < 7648$
   (b) Use 11: $\geq 311 \times 3 \times 11 = 10263 > 9999$.
4. If use 311, at least two 3's, and 11:
   $311 \times 11 \times 9 = 30789 > 9999$.
5. If use 311 and 9 does not work: $311 \times 2 \times 9 = 5598 < 7648$.
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:

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

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

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

But what do we mean by Factoring is Hard?

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

But what do we mean by Factoring is Hard?

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.

An Approach To Generating Random Bits

Random-number generation

1. Continually collect 'unpredictable" data.
2. This data may be biased.
3. Correct biases in it to make it more random.
4. Called smoothing.

Unpredictable: Different models.

1. Our Model: There is a $0 < p < 1$ such that each bit has
   $$\Pr(1) = p,\ \Pr(0) = 1 - p.$$
   Bits are independent. p is not known.
2. Simple dependency. For example, if $b_i = 1$ then $\Pr(b_{i+1} = 1) = p$.
3. Complicated dependencies. Depends on last x bits.

Smoothing via Von Neumann Technique (VN)

- Need to eliminate both *bias*.
- VN technique for eliminating bias:
  - Collect two bits per output bit
    - $01 \mapsto 0$
    - $10 \mapsto 1$
    - $00, 11 \mapsto$ skip
  - Note that this assumes *independence* (as well as constant bias)
  - This gives truly random bits but takes time.

How Many Random Bits Can We Expect?

Assume that $\Pr(b = 0) = p$ and $\Pr(b = 1) = 1 - p$.

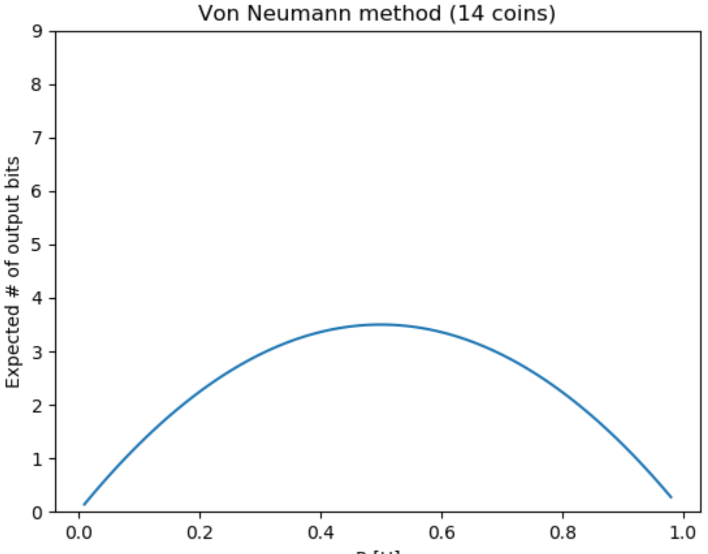
If flip 2 coins then expected numb of rand bits is

$$\Pr(01) + \Pr(10) = p(1 - p) + (1 - p)p = 2p(1 - p).$$

If flip $2n$ coins then expected number of rand bits is $2np(1 - p)$.

How Good is VN Method?

If flip 14 coins ($n = 7$) then we get the following graph:



Lets flip 4 Coins

VN method: flip 2 coins, if 00 or 11 then toss out.
If 01 then output 0, if 10 then output 1.
Note: Needed that $|\{01, 10\}| = 2^1$, a power of 2.

Lets flip 4 Coins

VN method: flip 2 coins, if 00 or 11 then toss out.
If 01 then output 0, if 10 then output 1.
Note: Needed that $|\{01, 10\}| = 2^1$, a power of 2.

EM method: flip 4 coins. If don't have 2 0's 2 1's then toss out. There are $\binom{4}{2} = 6$ possibilities. Whoops- not a power of 2. Toss out MORE to get to a power of 2. If 1100 or 1010 then toss out.
If 0011 then output 00
If 0101 then output 01
If 0110 then output 10
If 1001 then output 11

Why works: Within the 2 0's and 2 1's all equally likely.
Exp number of random bits: $2(4 \times p^2(1-p)^2) = 8p^2(1-p)^2$.

Can we do better with just 4 bits?

Lets flip 4 Coins

VN method: flip 2 coins, if 00 or 11 then toss out.
If 01 then output 0, if 10 then output 1.
Note: Needed that $|\{01, 10\}| = 2^1$, a power of 2.

EM method: flip 4 coins. If don't have 2 0's 2 1's then toss out. There are $\binom{4}{2} = 6$ possibilities. Whoops- not a power of 2. Toss out MORE to get to a power of 2. If 1100 or 1010 then toss out.
If 0011 then output 00
If 0101 then output 01
If 0110 then output 10
If 1001 then output 11

Why works: Within the 2 0's and 2 1's all equally likely.
Exp number of random bits: $2(4 \times p^2(1-p)^2) = 8p^2(1-p)^2$.

Can we do better with just 4 bits?Yes.

Lets Flip 4 Coins and Try to Use More Poss

ELIAS: flip 4 coins. If get one 1 then
If 0001 then output 00
If 0010 then output 10
If 0100 then output 01
If 1000 then output 11

If get two 1's then as on last slides.

If get three 1's then
If 1110 then output 00
If 1101 then output 01
If 1011 then output 10
If 0111 then output 11

Exp Number of Random bits

$$2(4p^2(1-p)^2 + 4p^3(1-p) + 4(1-p)^3p) =$$

$$8(p^2(1-p)^2 + p^3(1-p) + (1-p)^3p)$$

$$8((1-p)(p^2(1-p) + p^3 + (1-p)^2p))$$

Seven Coin Flips: 4 0's, 3 1's

Flip 7 coins. If you get 4 0's and 3 1's then of the Of the $\binom{7}{3} = 35$ possible strings toss 3 of them out to get down to $32 = 2^5$.
We choose to toss out 1110000, 1101000, 1100100.
If 0000111 then output 00000
If 0001011 then output 00001
If 0001101 then output 00010
If 0001011 then output 00011
If 0001110 then output 00100
If 0010011 then output 00101
$\vdots$
3 0's and 4 1's is similar.
Note: Get out 5 random bits.

Seven Coin Flips: 5 0's, 2 1's

Flip 7 coins. If you get 5 0's and 2 1's then of the Of the $\binom{7}{2} = 21$ possible strings toss 5 of them out to get down to $16 = 2^4$.
We choose to toss out 0001001, 0001010, 0001011, 0001100, 0001101.
If 0000011 then output 0000
If 0000101 then output 0001
If 0000110 then output 0011
If 0001001 then output 0100
If 0001010 then output 0101
$\vdots$
Note: Get out 4 random bits.

Elias Method for Seven Bits: Preprocessing

Flip 7 coins.

1. Of the $\binom{7}{3} = 35$ elts of $\{0,1\}^7$ with 4 0's and 3 1's, toss 3 of them out. Pick them at random (we always do that below). Let B be a bijection from whats left to $\{0,1\}^5$.
2. Of the $\binom{7}{3} = 35$ elts of $\{0,1\}^7$ with 3 0's and 4 1's, toss 3 of them out. Let B be a bijection from whats left to $\{0,1\}^5$.
3. Of the $\binom{7}{2} = 21$ elts of $\{0,1\}^7$ with 5 0's and 2 1's, toss 5 of them out. Let B be a bijection from whats left to $\{0,1\}^4$.
4. Of the $\binom{7}{2} = 21$ elts of $\{0,1\}^7$ with 2 0's and 5 1's, toss 5 of them out. Let B be a bijection from whats left to $\{0,1\}^4$.
5. Of the $\binom{7}{1} = 7$ elts of $\{0,1\}^7$ with 6 0's and 1 1's, toss 3 of them out. Let B be a bijection from whats left to $\{0,1\}^2$.
6. Of the $\binom{7}{1} = 7$ elts of $\{0,1\}^7$ with 1 0's and 6 1's, toss 3 of them out. Let B be a bijection from whats left to $\{0,1\}^2$.

Sequences tossed out are called bad. We specify B next slide.

Elias Method

Assume that $\Pr(b = 0) = p$ and $\Pr(b = 1) = 1 - p$.

1. Flip 7 coins. Let the sequence be s.
2. If s is bad then goto step 1.
3. Output $B(s)$. (could be 2,4, or 5 bits).

Let X be the number of bits.

Expected Number of Random Bits

$$E(X) = 5\Pr(X = 5) + 4\Pr(X = 4) + 2\Pr(X = 2)$$

$$5\Pr(X = 5) = 5 \times (32p^4(1 - p)^3 + 32p^3(1 - p)^4) = 160p^3(1 - p)^3$$

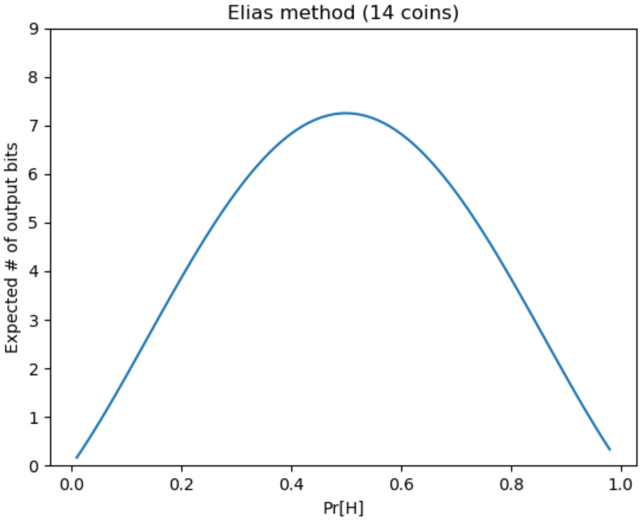
$4\Pr(X = 4) = 4 \times (16p^5(1 - p)^2 + 16p^2(1 - p)^5) =$
$64p^2(1 - p)^2(p^3 + (1 - p)^3)$

$$2\Pr(X = 2) = 2\times(4p^6(1-p)+4p(1-p)^6) = 8p(1-p)(p^5+(1-p)^5)$$

$$E(X) = -8p^6 + 24p^5 - 40p^3 + 16p^3 + 8p$$

How good is Elias Method

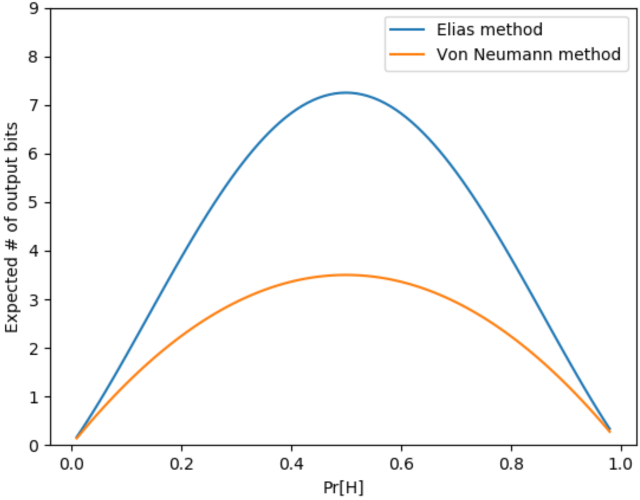
If flip 14 bits:



Much better than VN. Can we do better? Discuss.

VN vs GMS

If we flip 14 bits:



Is Elias Actually Used?

No

Discuss why

Is Elias Actually Used?

No

Discuss why

1. Assumes independent bits with constant bias.
2. Need to wait for all 7 flips to get some bits.
3. If $p = 0.3$ then 14 flips yields only ~ 4 random bits.

Is Elias Actually Used?

No

Discuss why

1. Assumes independent bits with constant bias.
2. Need to wait for all 7 flips to get some bits.
3. If $p = 0.3$ then 14 flips yields only ~ 4 random bits. Can improve this but not by much.

Is Elias Actually Used?

No

Discuss why

1. Assumes independent bits with constant bias.
2. Need to wait for all 7 flips to get some bits.
3. If $p = 0.3$ then 14 flips yields only ~ 4 random bits. Can improve this but not by much.
4. Perfect randomness not really needed. Only need random-looking to Eve.

Other Ciphers That Were Actually Used

The Playfair Cipher

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 Grid and the First Case

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

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: 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:
   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

The Rail Fence Cipher as Understood When Invented

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

The Rail Fence Cipher as Understood When Invented

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
1st letter, 5th letter, 9th letter,
2nd letter, 4th letter, 6th letter, 8th letter, 10th letter,
3rd letter, 7th letter, 11th letter.
Leave as an exercise what happens if k rows, n letter message.

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

The AutoKey Cipher: A Variant of Vigenere

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 just revealed for Vig key.

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 Vigenere cipher.

Marina's Opinion (TA)

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. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".

Marina's Opinion (TA)

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. Maybe there isn't any. I feel like they are arbitrary methods that seem "fun" and "complicated".

Is she right?

Marina's Opinion (TA)

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. 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)

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. 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)

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. 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)

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. 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)

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. 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, whose going to know?

Marina's Opinion (TA)

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. 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, whose going to know?

That could be why Playfair was not cracked!

Marina's Opinion (TA)

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. 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, whose going to know?

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