An Easy to Understand Introduction to Encryption:

or how I learned to stop worrying and love `iMiUERyPa2L6iXTfH+DS6A==`

Rotem Guttman

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0597

Easy to understand introduction to Encryption

- **Who am I?**
- **Disclaimer**
- **What is encryption?**

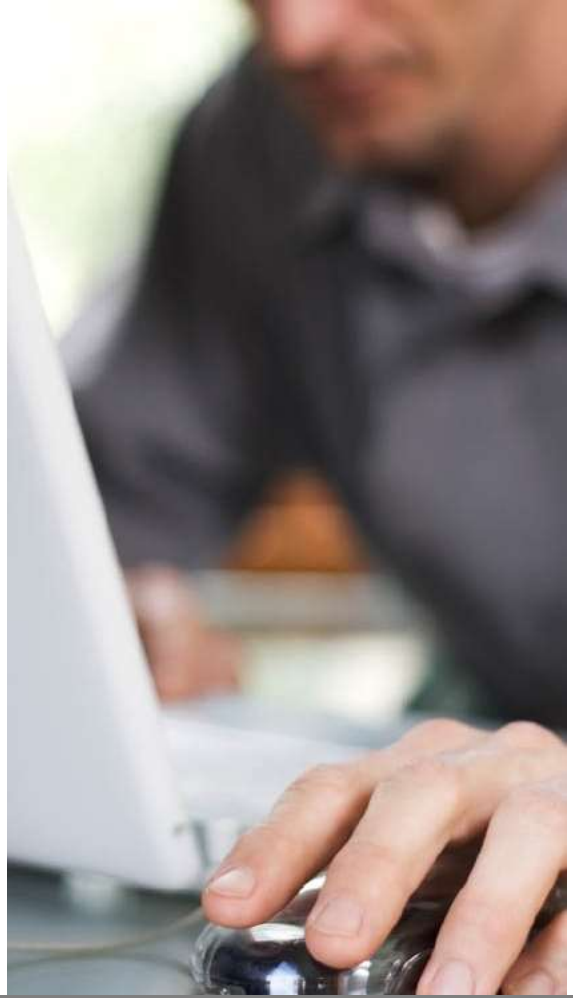
Who Am I?

My Jobs

- Cybersecurity Researcher
  - Carnegie Mellon University, Software Engineering Institute, CERT Division
- Adjunct Faculty
  - Carnegie Mellon University, Information Networking Institute

Disclaimer

(Not the legal kind)



Disclaimer

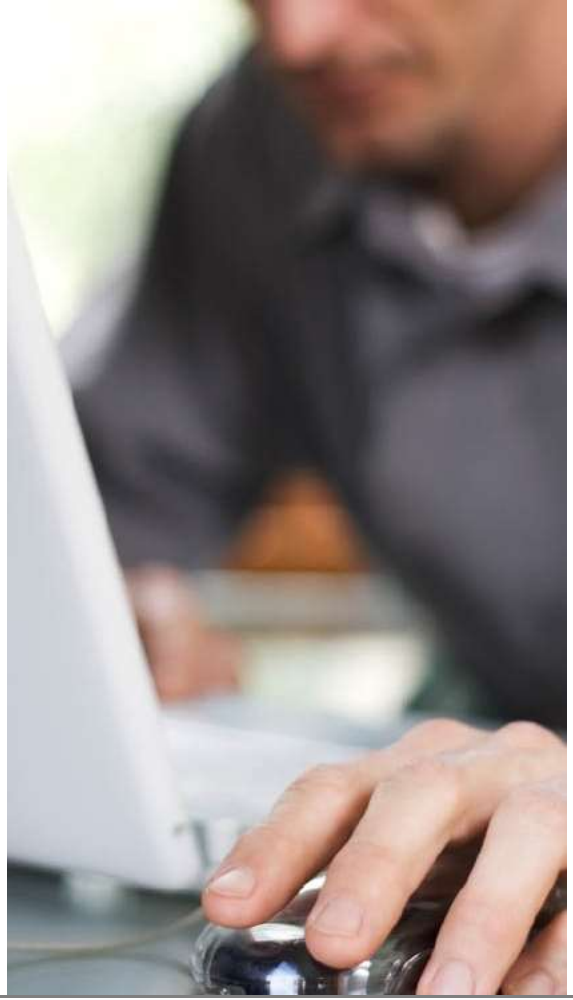
This talk is aimed at a nontechnical audience and contains numerous simplifications and generalizations meant to convey complex subject matter in an understandable manner within the time constraints available.

Anyone wishing to fully understand the theory, practice, and implementation details of all modern encryption schemes is welcome to contact me after the presentation.

(Warning: Please allow 6-8 years of full time study to cover this material)

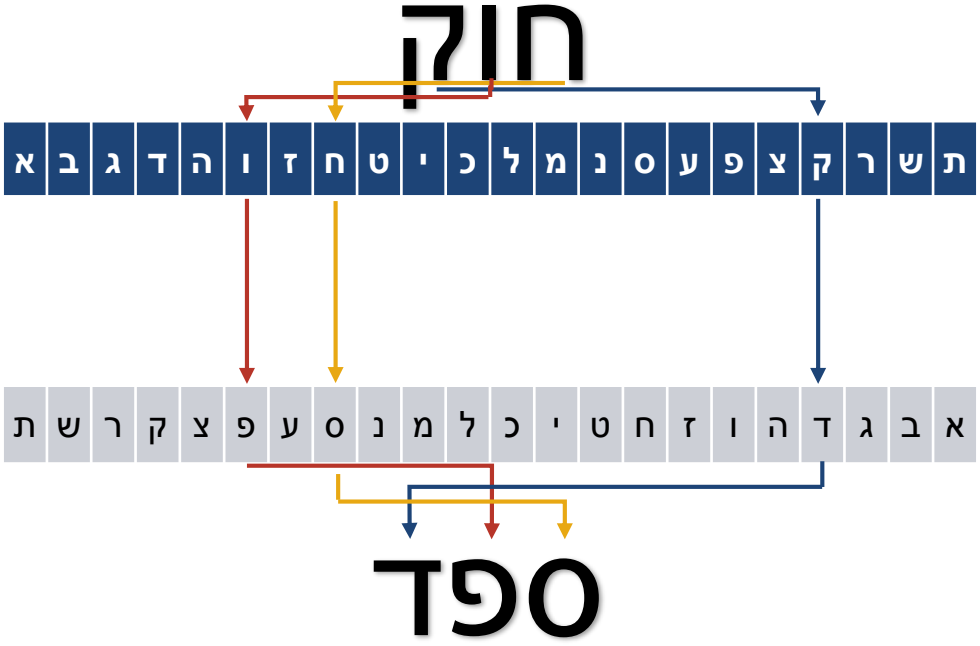
What Encryption Is

History



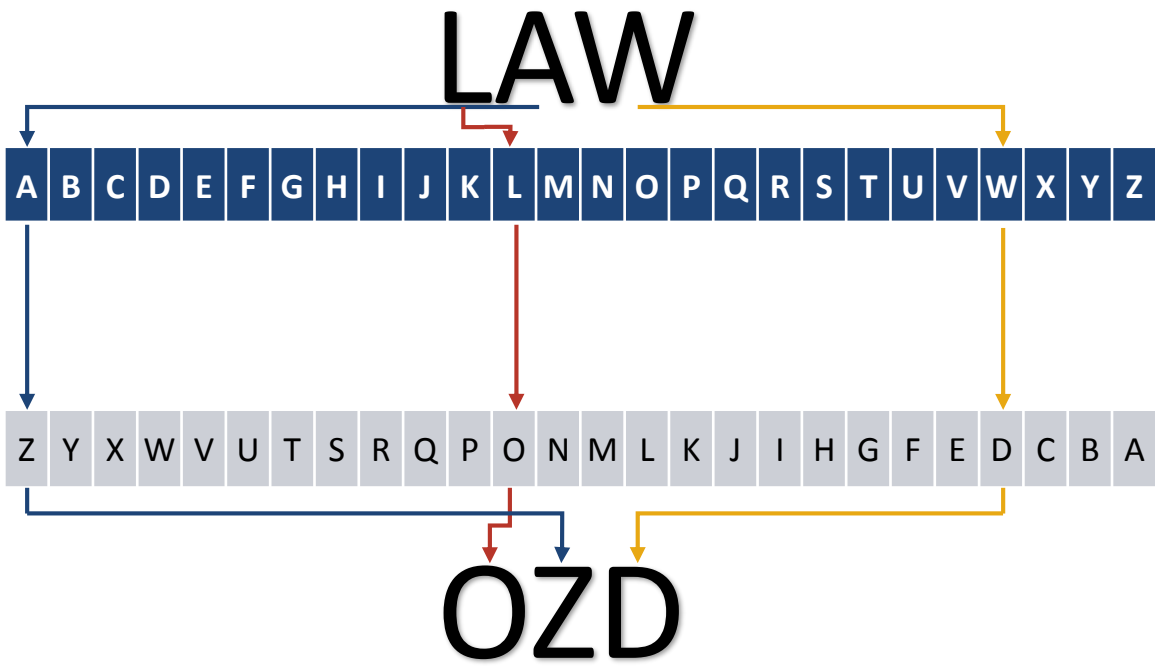
History

- Extremely long history!
  - At least since 1500 BC
- Substitution Cyphers
  - אתבש
  - Caesar Rotation
- Transposition Cyphers
  - Skytale



History

- Extremely long history!
  - At least since 1500 BC
- Substitution Cyphers
  - אתבש
  - Caesar Rotation
- Transposition Cyphers
  - Skytale



History

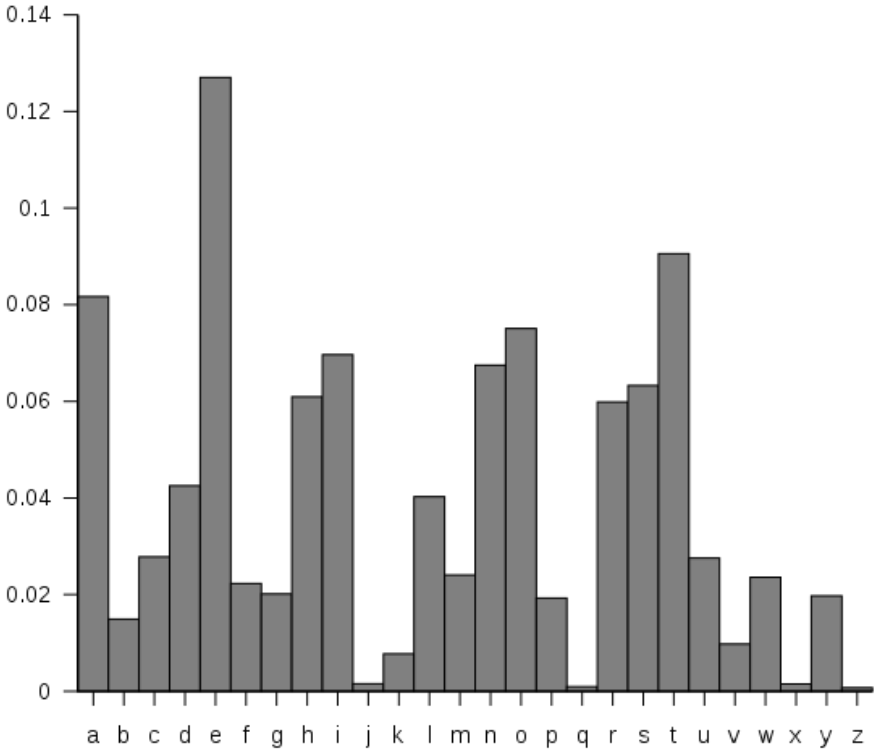
- Extremely long history!
  - At least since 1500 BC
- Substitution Cyphers
  - אתבש
  - Caesar Rotation
- Transposition Cyphers
  - Skytale

History

- Extremely long history!
  - At least since 1500 BC
- Substitution Cyphers
  - אתבש
  - Caesar Rotation
- Transposition Cyphers
  - Skytale

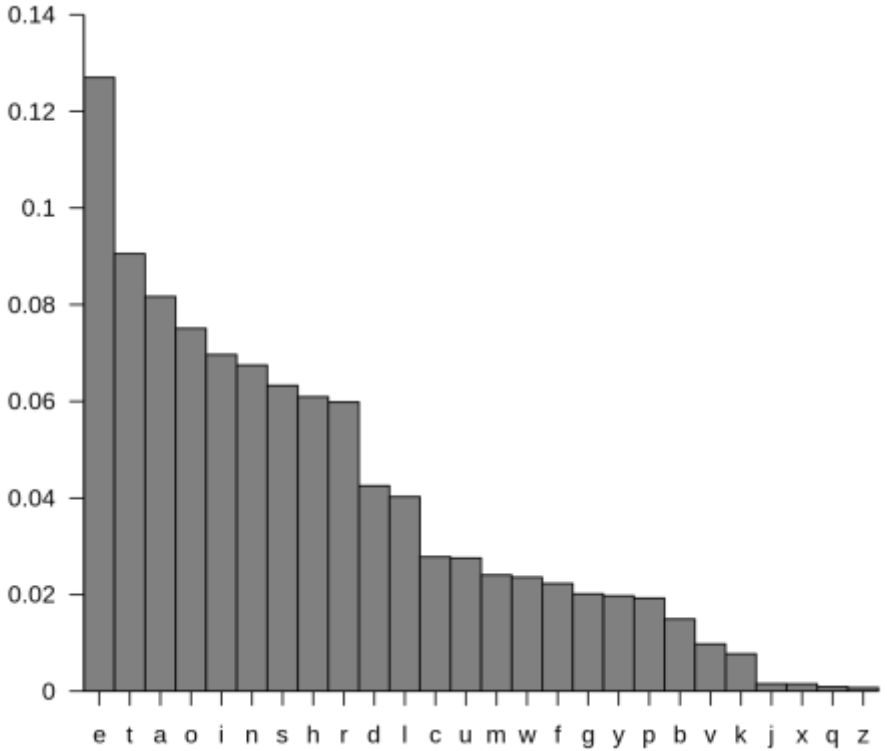
History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace



History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace



History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

Ol beqre bs gur xvat

lbh ner gb zbir gur guveq ertvzrag

bs gur nezl gb gur abegu fuber

ng gur oernx bs qnja

History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

Ol beqre bs **gur** xvat

lbh ner gb zbir **gur** guveq ertvzrag

bs **gur** nezl gb **gur** abegu fuber

ng **gur** oernx bs qnja

History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

GUR = THE?

Ol beqre bs **gur** xvat

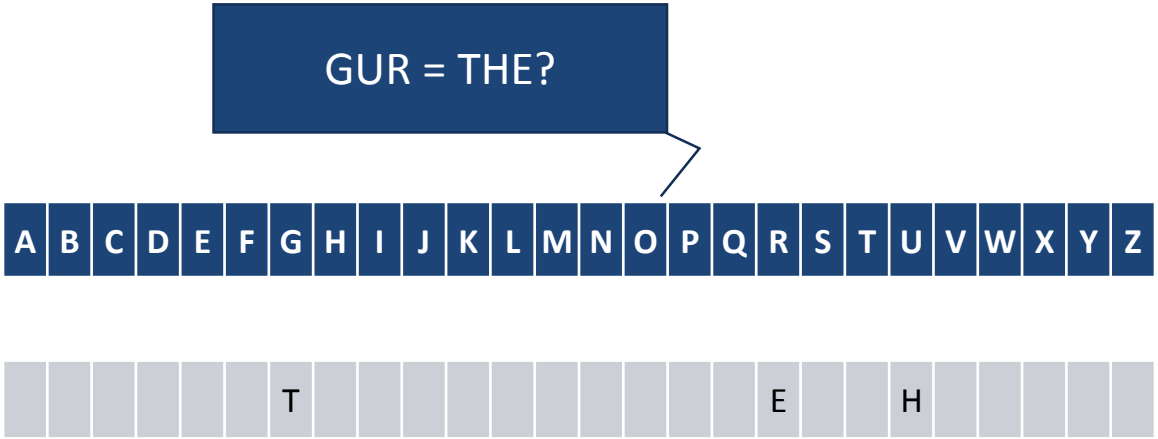
lbh ner gb zbir **gur** guveq ertvzrag

bs **gur** nezl gb **gur** abegu fuber

ng **gur** oernx bs qnja

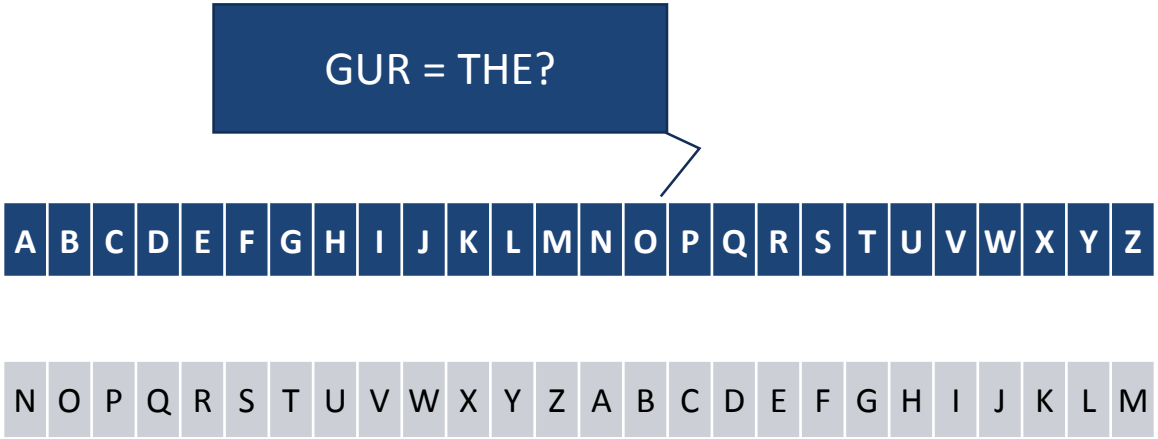
History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace



History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace



History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

GUR = THE?

Ol beqre bs **gur** xvat

lbh ner gb zbir **gur** guveq ertvzrag

bs **gur** nezl gb **gur** abegu fuber

ng **gur** oernx bs qnja

History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

GUR = THE?

Ol beqre bs **gur** xvat

lbh ner gb zbir **gur** guveq ertvzrag

bs **gur** nezl gb **gur** abegu fuber

ng **gur** oernx bs qnja

History

- Easily Broken
  - “Hey, nice belt”
  - Frequency analysis
    - Longer Messages
      - Trend to average
      - Short words
  - Limited keyspace

GUR = THE?

By order of **the** king

you are to move **the** third regiment

of **the** army to **the** north shore

at **the** break of dawn

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

Tabula Rasa (English)

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

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

Message: “BY ORDER OF THE KING YOU ARE TO…”

Keyphrase: “KING MIDAS”

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

Message: “BY ORDER OF THE KING YOU ARE TO…”

Keystream: “ KI NGMID AS KIN GMID ASK ING MI”

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

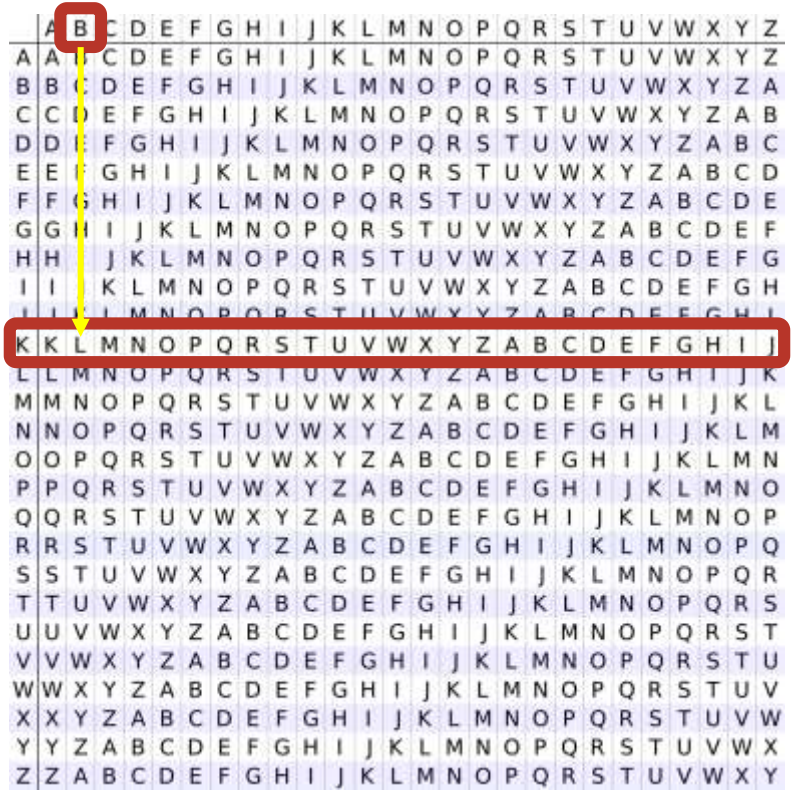
Message: “BY ORDER OF THE KING YOU ARE TO…”

Keystream: “ KI NGMID AS KIN GMID ASK ING MI”

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

Tabula Rasa (English)



History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

But Wait! Notice Something?

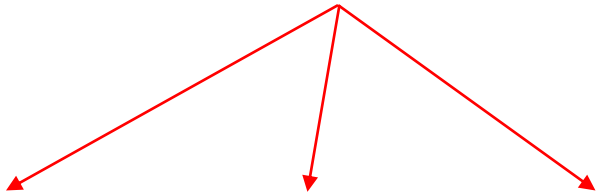
Message: “BY ORDER OF THE KING YOU ARE TO…”

Keystream: “ KI NGMID AS KIN GMID ASK ING MI”

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

But Wait! Notice Something?



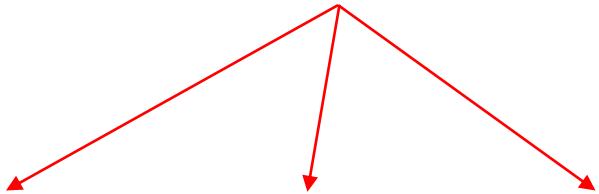
Message: “BY ORDER OF THE KING YOU ARE TO…”

Keystream: “ KI NGMID AS KIN GMID ASK ING MI”

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

But Wait! Notice Something?



Message: “BY ORDER OF THE KING YOU ARE TO…”

Keystream: “ KI NGMID AS KIN GMID ASK ING MI”

Repeated instances map to the same row. Effectively just N different messages using N different substitution cyphers!

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

Keystream repetition breaks the code

- Don’t let the keystream repeat. Make the keystream as long as the message.

Guessing the keystream breaks the code

- Randomly generate the keystream so it can’t be guessed

History

- Vigenère cipher
  - Uses Keyphrase
    - Keyphrase is repeated
  - Lookup proper row in tabula rasa based on keyphrase letter

- What if…
- Keystream never repeats
- Keystream is randomly generated
- Keystream is never reused
- Keystream is never disclosed (destroyed after use)

= One Time Pad

History

- One time pad
  - Provably unbreakable
  - The platinum standard
  - Nearly impossible in practice
    - Key Distribution
    - Randomness

- Conditions which break a one time pad
  - Stream not random
  - Reuse
  - Time travel
  - Telepathy
  - Magic

History

- One time pad
  - Provably unbreakable
  - The platinum standard
  - Nearly impossible in practice
    - Key Distribution
    - Randomness

- Not on that list:
  - Number of symbols in alphabet

What is the alphabet in a computer?

- Binary! (0's and 1's)

History

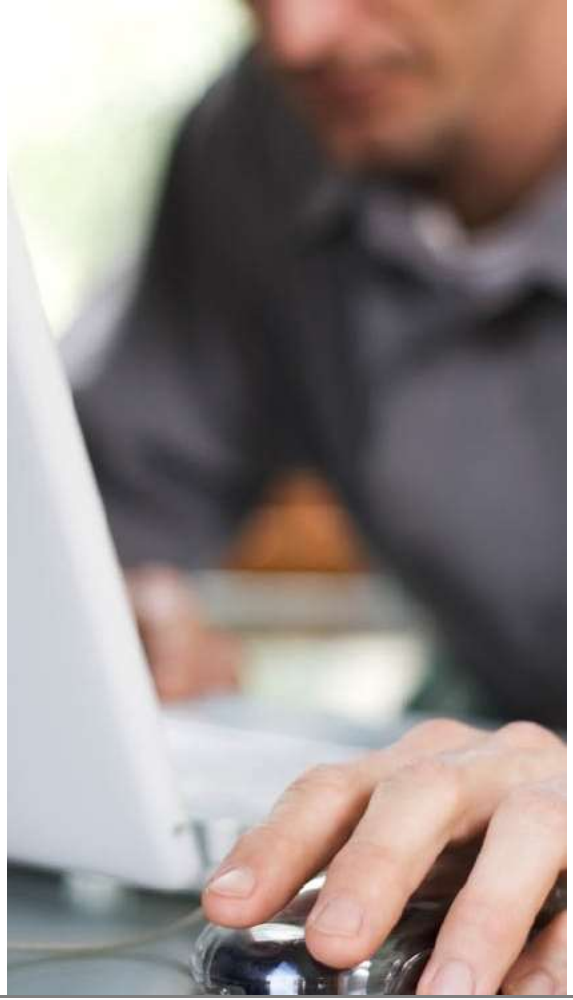
- Really small alphabet
  - Tiny Tabula Rasa

Tabula Rasa for Binary Alphabet

	0	1
0	0	1
1	1	0

What Encryption Is

XOR



XOR

- Flip only the marked bits

Message	1011	1101	1010	1011
Keystream	1010	0101	1100	0010
XOR	⊕	⊕	⊕	⊕
Result	0001	1000	0110	1001

XOR

- Reversable
  - Just XOR it again!

Result	0001	1000	0110	1001
Keystream	1010	0101	1100	0010
XOR	⊕	⊕	⊕	⊕
Message	1011	1101	1010	1011

XOR

- Truth Table

Truth Table for the XOR function

	0	1
0	0	1
1	1	0

XOR

- Truth Table

Truth Table for the XOR function

	0	1
0	0	1
1	1	0

History

- Really small alphabet
  - Tiny Tabula Rasa

Tabula Rasa for Binary Alphabet

	0	1
0	0	1
1	1	0

XOR based (symmetric) encryption

Sender:

- Takes input (Plaintext)
- XORs with keystream
- Sends output (Cipher Text)

Receiver:

- Takes input (Cipher Text)
- XORs with keystream
- Receives output (Plaintext)

But how do we agree on the keystream?

- Generate it the same way
  - Pseudo-random generator based on a seed value
  - Must agree on the seed

Note: Pseudo-Random ≠ Random

No longer impossible to break

If I can guess your seed, I can read your data.

Symmetric vs. Asymmetric

So how do I send the seed?!

- Chicken and the egg problem!

Solution: Asymmetric Encryption

- Symmetric Encryption
  - Encrypt and Decrypt use the same key
- Asymmetric Encryption
  - Encrypt and Decrypt use different keys
  - Think of it as:
    - A lockbox (encryption key)
    - A key (decryption key)

Asymmetric encryption

So how do I send the seed?!

- Chicken and the egg problem!

Solution: Asymmetric Encryption

- Can give anyone the lock box
- Can give everyone the same lock box
- They lock the seed in it
- Only I can open it

Asymmetric encryption

Why not use only Asymmetric encryption?

- More computationally expensive
- Harder to secure due to relationship between keys
  - Requires more bits
    - Roughly equivalent:
      - 128 bit symmetric
      - 2048 bit asymmetric