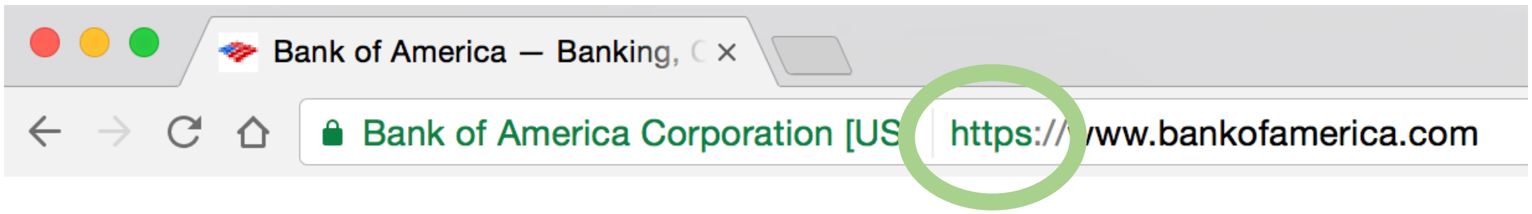
COS433/Math 473: Cryptography

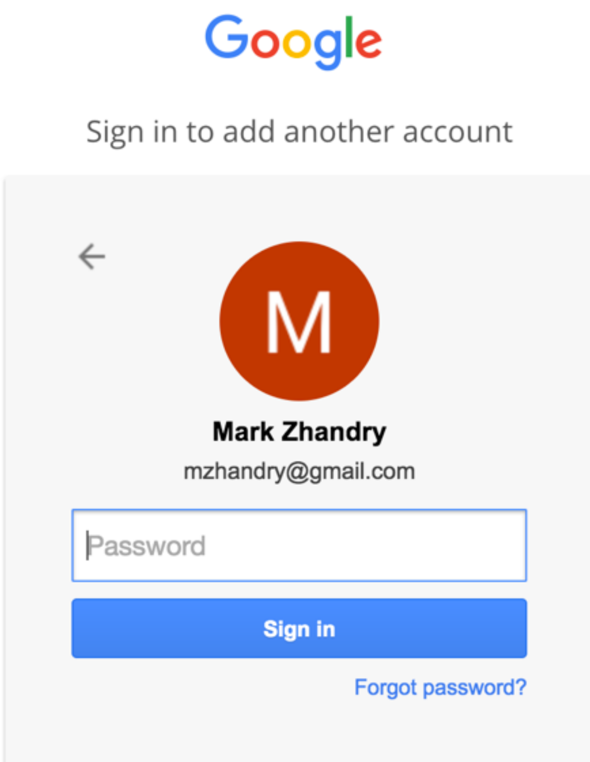
Mark Zhandry

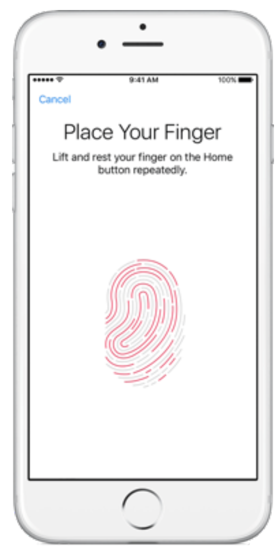
Princeton University

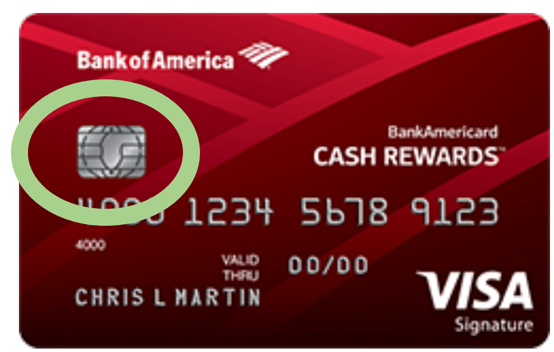
Spring 2017

Cryptography Is Everywhere









A Long & Rich History

Examples:

- ~50 B.C. – Caesar Cipher
- 1587 – Babington Plot
- WWI – Zimmermann Telegram
- WWII – Enigma
- 1976/77 – Public Key Cryptography
- 1990's – Widespread adoption on the Internet

Increasingly Important

WIRED SUBSCRIBE

BRIAN BARRETT SECURITY 03.30.16 7:00 AM

THE APPLE-FBI BATTLE IS OVER, BUT THE NEW CRYPTO WARS HAVE JUST BEGUN

THE FRIDAY COVER

How to Hack an Election in 7 Minutes

With Russia already meddling in 2016, a ragtag group of obsessive tech experts is warning that stealing the ultimate prize—victory on Nov. 8—would be child's play.

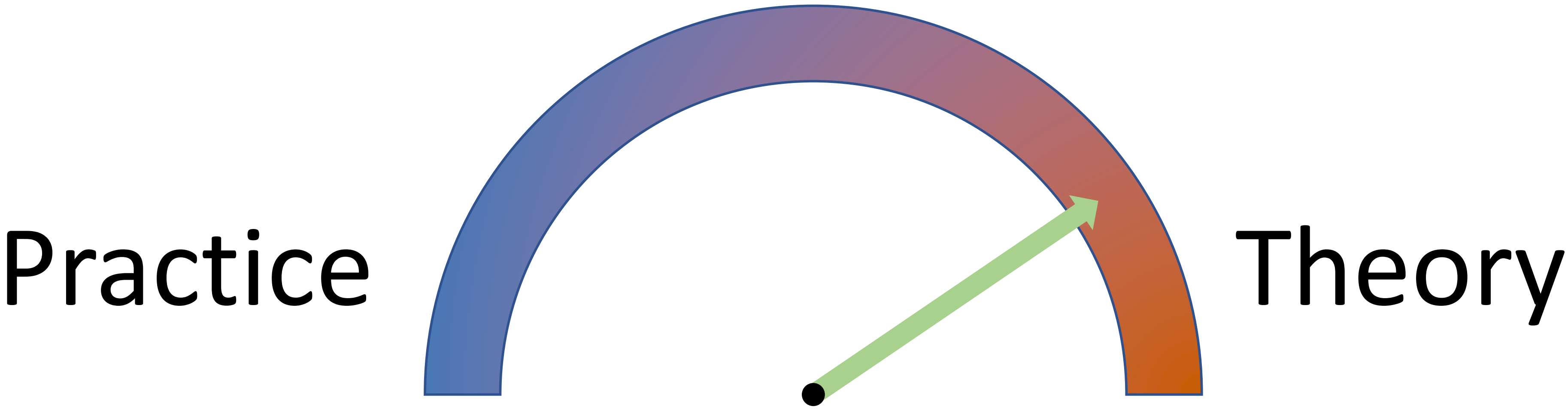
By BEN WOFFORD | August 05, 2016

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 09.22.16 12:15 PM

HACK BRIEF: YAHOO BREACH HITS HALF A *BILLION* USERS

COS 433



Inherent to the study of crypto

- Working knowledge of fundamentals is crucial
- Cannot discern security by experimentation
- Proofs, reductions, probability are necessary

COS 433

What you should expect to learn:

- Foundations and principles of modern cryptography
- Core building blocks
- Applications

Bonus:

- Debunking some Hollywood crypto
- Better understanding of crypto news

COS 433

What you will **not** learn:

- Hacking
- Crypto implementations
- How to design secure **systems**
- Viruses, worms, buffer overflows, etc

Administrivia

Course Information

Instructor: Mark Zhandry (mzhandry@p)
TA: Fermi Ma (fermima1@g)

Lectures: MW 1:30-2:50pm

Webpage: cs.princeton.edu/~mzhandry/2017-Spring-COS433/

Office Hours: please fill out Doodle poll

Piazza

piazza.com/princeton/spring2017/cos433mat473_s2017

Main channel of communication

- Course announcements
- Discuss homework problems with other students
- Find study groups
- Ask content questions to instructors, other students

Prerequisites

- Ability to read and write mathematical proofs
- Familiarity with algorithms, analyzing running time, proving correctness, O notation
- Basic probability (random variables, expectation)

Helpful:

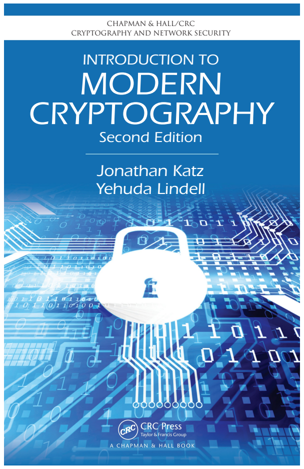
- Familiarity with NP-Completeness, reductions
- Basic number theory (modular arithmetic, etc)

Reading

No required text

If you want a text to follow along with:

<u>Introduction to Modern Cryptography</u>
by Katz, Lindell



For each lecture, page numbers for 2nd edition will be posted on course website

Grading

50% Homeworks
- 1 per week
- Drop lowest 2
- Occasional extra credit problems
- Collaboration encouraged, but write up own solutions

20% Take-home Midterm
- Sometime during midterms week, TBA
- Done individually

30% Take-home Final

Classroom Policies

Please stop me if you have any questions

Please come to class to be engaged and to learn

- Notes for each lecture will be added to the webpage
- I don’t take attendance
- Don’t be on Facebook, working on assignments, etc

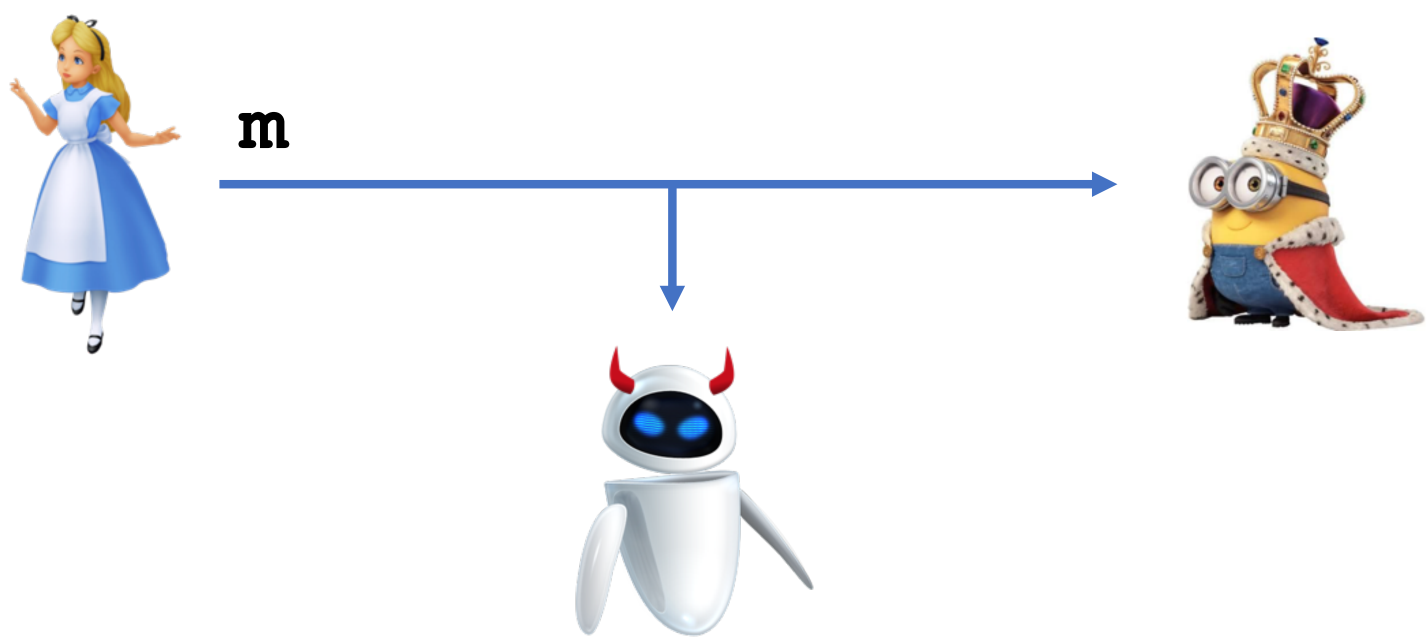
Feel free to call me “Mark”, “Professor”, “Hey You”, etc, though “Mark” is preferred

Today:
A Brief (Non-Linear) History of Cryptography

Pre-modern Cryptography

1900 B.C. – mid 1900's A.D.

With few exceptions, synonymous with **encryption**



Pre-modern Cryptography

1900 B.C. – mid 1900's A.D

With few exceptions, synonymous with **encryption**

k

`c = Enc(k,m)`

k

`m = Dec(k,c)`

For our discussions, assume **`Enc`**, **`Dec`** known, only **`k`** is secret

1900 BC: “Protocrypto”

Inscriptions on monuments to Egyptian pharaohs

- First deliberate transformation of writing
- Method: substitution of hieroglyphs
- Goal: prestige, authority, intrigue

500 B.C. – Atbash Cipher

Alphabet reversal

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

For English alphabet

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

Example:

plaintext: **super secret message**

ciphertext: **HFKVI HVXIVG NVHHZTV**

50 B.C. – Caesar Cipher

Used by Julius Caesar

Alphabet shift by 3

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
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

Example:

plaintext: **super secret message**

ciphertext: **VXSHU VHFUHW PHVVDJH**

Atbash, Caesar not true ciphers: what's the secret key?

Generalization: Shift Ciphers

Shift by fixed, secret increment (**`k = 0,…,25`**)

Some examples:

- Shift by 1: Augustus Caesar; Jewish mezuzah
- Shift by 3: Caesar Cipher
- Shift by 13: ROT13

Sometimes also called “Caesar ciphers”

Security of Shift Ciphers?

Problem: only 26 possibilities for key

“Brute force” attack:

- Try all 26 possible shifts
- For each shift, see if something sensible comes out

Example Brute Force Attack

Ciphertext: **HJETG HTRGTI BTHHPVT**

Key	Plaintext
0	HJETG HTRGTI BTHHPVT
1	IKFUH IUSHUJ CUIIQWU
2	JLGVI JVTIVK DVJJRXV
3	KMHWJ KWUJWL EWKKSYW
4	LNIXK LXVKXM FXLLTZX
5	MOJYL MYWLYN GYMMUAY
6	NPKZM NZXMZO HZNNVBZ
7	OQLAN OAYNAP IAOOWCA
8	PRMBO PBZOBQ JBPPXDB
9	QSNCP QCAPCR KCQQYEC
10	RTODQ RDBQDS LDRRZFD
11	SUPER SECRET MESSAGE
12	TVQFS TFDSFU NFTTBHF

Key	Plaintext
13	UWRGT UGETGV OGUUCIG
14	VXSHU VHFUHW PHVVDJH
15	WYTIV WIGVIX QIWWEKI
16	XZUJW XJHWJY RJXXFLJ
17	YAVKX YKIXKZ SKYYGMK
18	ZBWLY ZLJYLA TLZZHNL
10	ACXMZ AMKZMB UMAAIOM
20	BDYNA BNLANC VNBBJPN
21	CEZOB COMBOD WOCCKQO
22	DFAPC DPNCPE XPDDLRP
23	EGBQD EQODQF YQEEMSQ
24	FHCRE FRPERG ZRFFNTR
25	GIDSF GSQFSH ASGGOUS

Security of Shift Ciphers?

Problem: only 26 possibilities for key

"Brute force" attack:

- Try all 26 possible shifts
- For each shift, see if something sensible comes out

To avoid brute force attacks, need large key space

- On modern hardware, typically need #(keys) ≥ 2^{80}

(Often use #(keys) = 2^{128} or 2^{256})

Generalization: Substitution Ciphers

Apply fixed permutation to plaintext letters

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

Example:

plaintext: **`super secret message`**

ciphertext: **`ARQYV AYSVYX EYAAFJY`**

Number of possible keys?

$26! \approx 2^{88}$ ➡ brute force attack very expensive

Variation: Polybius Square

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

plaintext: `s u p e r  s e c r e t  m e s s a g e`

ciphertext: `4345351542 431513421544 32154343112215`

Keyed Polybius Square

	1	2	3	4	5
1	y	n	r	b	f
2	d	l	w	o	g
3	s	p	a	t	k
4	h	v	ij	x	c
5	q	u	z	e	m

plaintext: `s u p e r  s e c r e t  m e s s a g e`

ciphertext: `3152325413 315445135434 55543131332554`

Keyed Polybius Square

	1	2	3	4	5
1	y	n	r	b	f
2	d	l	w	o	g
3	s	p	a	t	k

Equivalent to plain substitution + unkeyed Polybius

- No security advantage over plain substitution

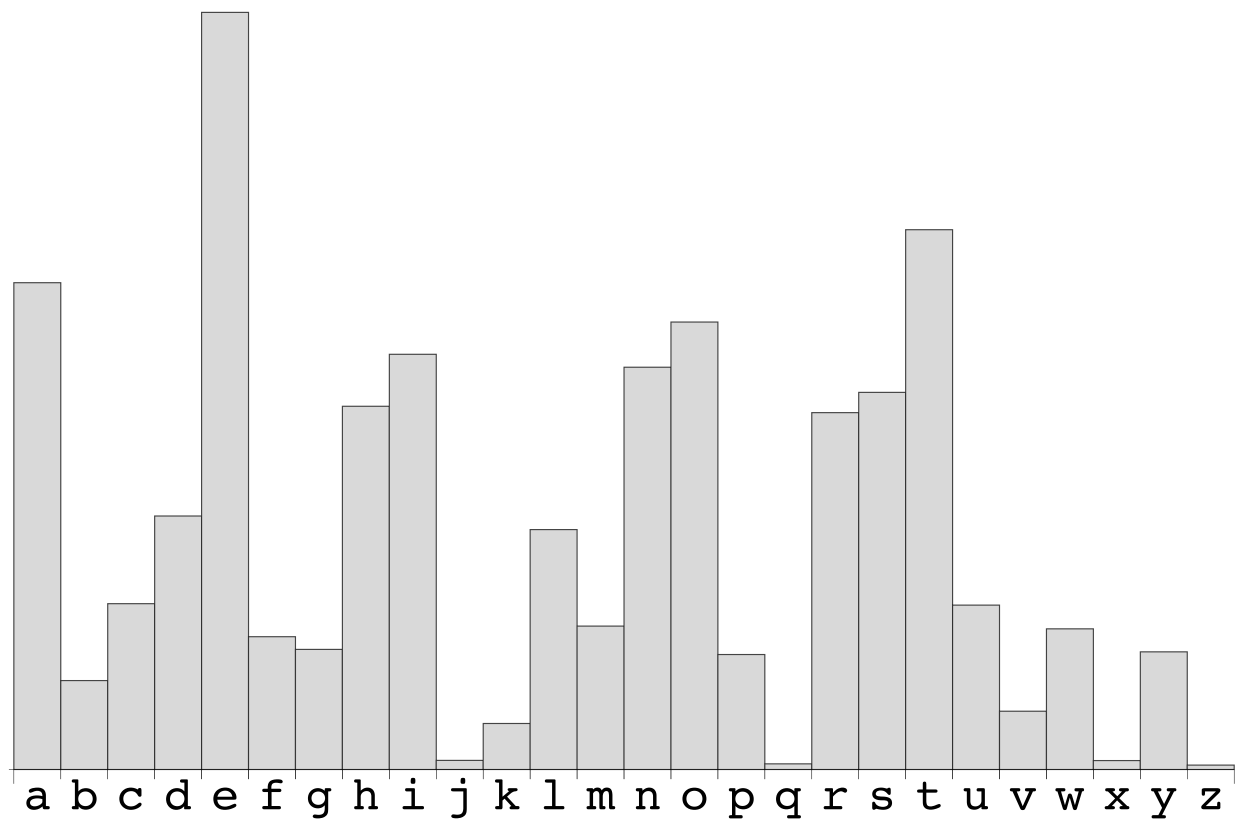
Instead, conceived for ease of transmission

- Signal messages by pairs of sets of torches
- Tapping on prison walls

800’s A.D. – First Cryptanalysis

Al-Kindi – Arab philosopher in modern-day Iraq

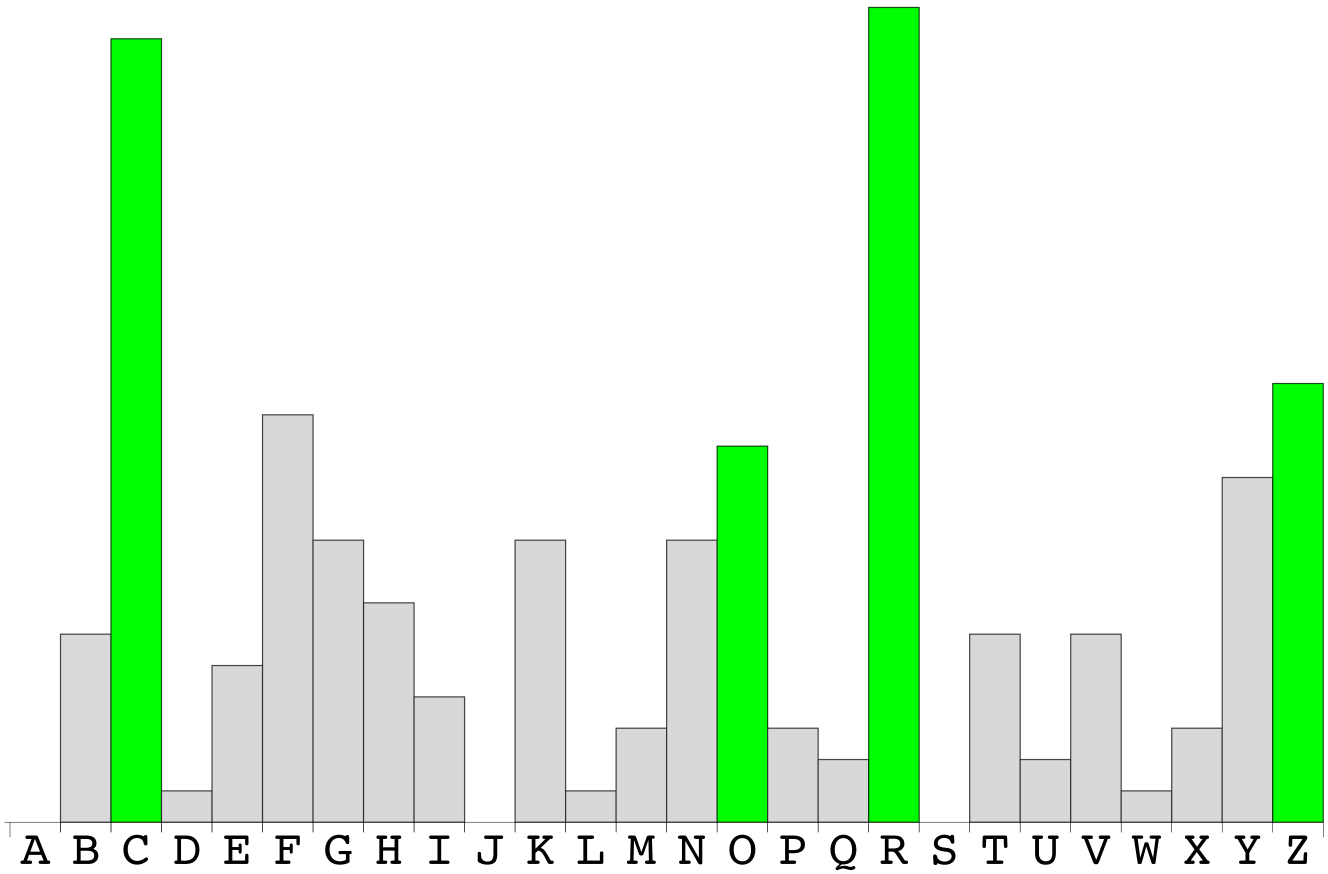
- Some characters are more common than others



Example

BOFC HNR Z NHMNCYCHCYOF KYIVRG CO RFKOBR NRFNYCYPR BZCZ, RPRF CVOHXV CVRE ZGR GRNYTYRFC CO Z MGHCR WOGKR ZCCZKU. YFBRRB, ME KOHFCYFX TRCCRGN ZFB KODIZGYFX CO CEIYKZT CRQC, EOH KZF GRKOPRG CVR ITZYFCRQC ZN LRTT ZN CVR URE

Example



Reasonable conjecture:

e→R, t→C, a→Z, o→O

Example

```
BoFt HNe a NHMNtYtHtYoF KYIVeG to eFKoBe
NeFNYtYPe Bata, ePeF tVoHXV tVeE aGe
GeNYTYeFt to a MGHte WoGKe attaKU.
YFBeeB, ME KoHFtYFX TetteGN aFB KoDIaGYFX
to tEIYKaT teQt, EoH KaF GeKoPeG tVe
ITaYFteQt aN LeTT aN tVe UeE
```

Maybe "**data**"? Maybe "**attack**"? Probably "**the**"

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
Z				R										O					C						

Example

doFt HNe a NHMNtYtHtYoF cYIheG to eFcode
NeFNYtYPe data, ePeF thoHXh theE aGe
GeNYTYeFt to a MGHte WoGce attack.
YFdeed, ME coHFtYFX TetteGN aFd coDIaGYFX
to tEIYcaT teQt, EoH caF GecoPeG the
ITaYFteQt aN LeTT aN the keE

"encode"?

"and"?

"as"?

"are"?

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
Z		K	B	R			V			U				O					C						

Example

"use"?

dont Hse a sHMstYtHtYon cYIher to encode sensYtYPe data, ePen thoHXh theE are resYTYent to a MrHte Worce attack. Yndeed, ME coHntYnX TetteGs and coDIarYnX to tEIYcaT teQt, EoH can recoPer the ITaYnteQt as LeTT as the keE

"indeed"? "even"? "force"? "recover"?

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
Z		K	B	R			V			U			F	O			G	N	C						

Example

dont use a suMstitution ciIher to encode sensitive data, even thouXh theE are resiTient to a Mrute force attack. indeed, ME countinX Tetters and coDIarinX to tEIicaT teQt, Eou can recover the ITainteQt as LeTT as the keE

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
Z		K	B	R	W		V	Y		U			F	O			G	N	C	H	P				

Example

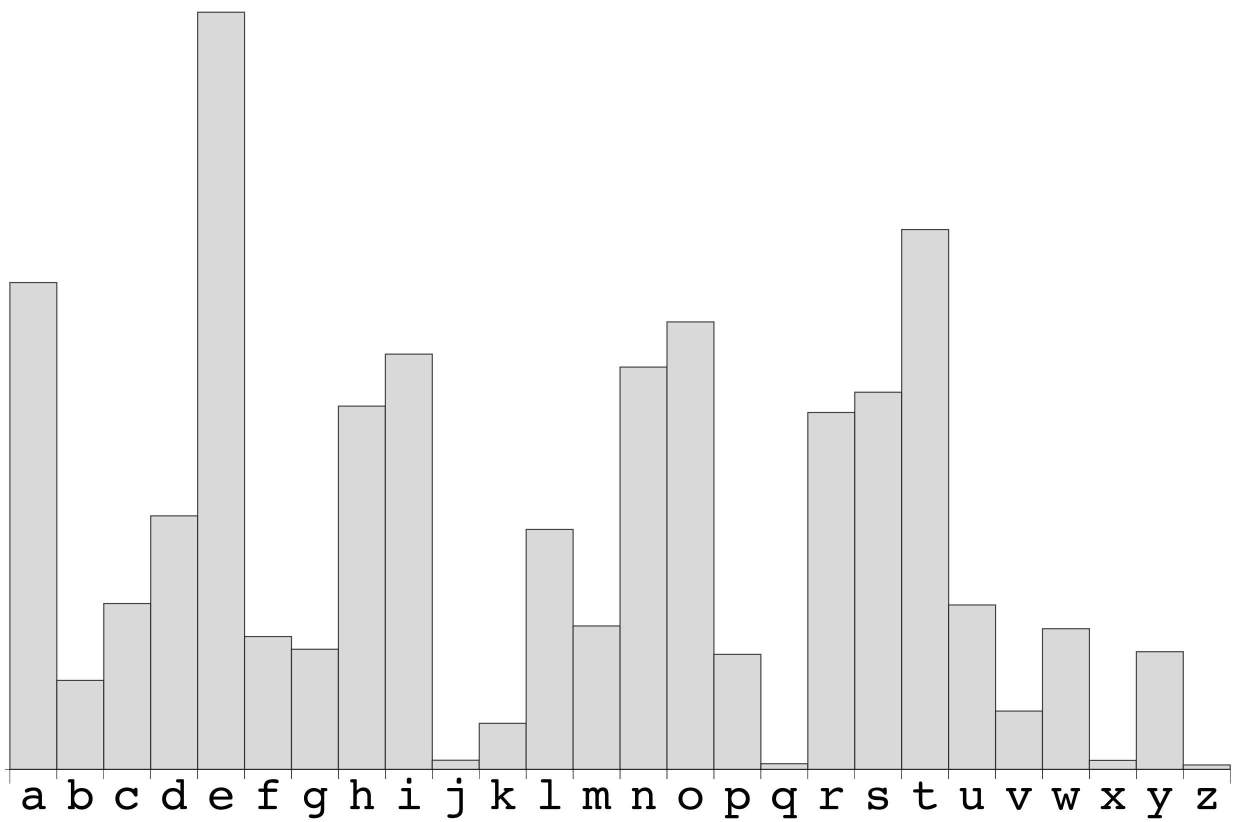
```
dont use a substitution cipher to encode
sensitive data, even though they are
resilient to a brute force attack.
indeed, by counting letters and comparing
to typical text, you can recover the
plaintext as well as the key
```

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

Defending Against Frequency Analysis

Problem

Differing letter frequencies reveal a lot



Polygraphic Substitution

Frequency analysis requires seeing many copies of the same character/group of characters

Idea: encode **$d= 2,3,4$**, etc characters at a time

- Effectively increase alphabet size to $\mathbf{26^d}$
- Number of repeats seen goes down
  - Most common digram: "th", 3.9%
    trigram: "the", 3.5%
    quadrigram: "that", 0.8%
- Require much larger ciphertext to perform frequency analysis

Polygraphic Substitution

Example: Playfair cipher

- Invented by Sir Charles Wheatstone in 1854
- Used until WWII

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

Polygraphic Substitution

Example: Playfair cipher

- Invented by Sir Charles Wheatstone in 1854
- Used until WWII

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

TH

- To encode, choose opposite corners of rectangle

Polygraphic Substitution

Example: Playfair cipher

- Invented by Sir Charles Wheatstone in 1854
- Used until WWII

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

TH → XS

- To encode, choose opposite corners of rectangle
- Additional rules for repeats, digrams in same row, etc

Polygraphic Substitution

Limitations:

- For small **d**, frequency analysis still possible by looking at common sequences of **d** characters
- For large **d**, either
  - Uniform random permutation. Needs $> 26^d$ bits to write down key
  - Restricting class of permutations may yield manageable key, but this may start introducing attacks
    - Later on in the course, we will see how to make this work

Homophonic Substitution

Ciphertexts use a larger alphabet

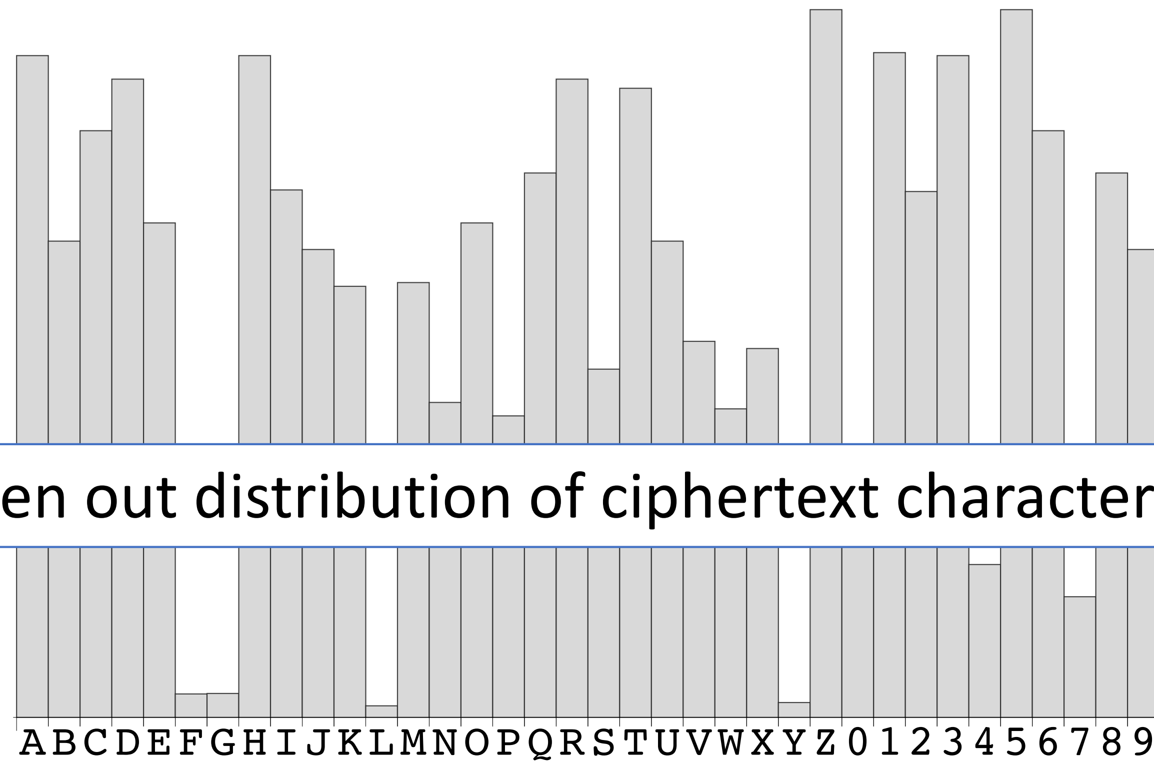
Common letters have multiple encodings

To encrypt, choose encoding at random

plaintext: **`super secret message`**
ciphertext: **`EKPH9 O3MJ3Z VAOEDNH`**

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
D	0	M	1	A	S	N	U	Q	G	7	T	V	I	6	P	Y	9	E	Z	K	4	X	F	W	L
R				H			B	8					2	C			J	O	5						
				3																					

Homophonic Substitution



Even out distribution of ciphertext characters

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
D	0	M	1	A	S	N	U	Q	G	7	T	V	I	6	P	Y	9	E	Z	K	4	X	F	W	L
R				H			B	8					2	C			J	O	5						
				3																					

Homophonic Substitution

In principle, by using sufficiently large ciphertext alphabet, character frequencies can be made ≈uniform

Thwarts vanilla frequency analysis

However, still possible to break
- Frequency analysis on pairs/groupings of letters

Homophonic Substitution

Example: “Grand Chiffre” (Great Cipher)

- Developed in 1600’s, used by Louis XIV
- Remained unbroken for 200 years
- Combination of polygraphic and homophonic
- 1890’s - finally cracked by Étienne Bazeries
  - Guessed that “`124-22-125-46-345`” stood for “`les ennemies`”
  - From there, things unraveled

Homophonic Substitution

Example: Copiale cipher

- 105-page encrypted book written in 1730's
- Secret society of German ophthalmologists
- Not broken until 2011 with help of computers

Polyalphabetic Substitution

Use a different substitution for each character

Example: Vigenère cipher

- Sequence of shift ciphers defined by keyword

keyword:	**crypt ocrypt ocrypto**
plaintext:	**super secret message**
ciphertext:	**ULNTK GGTPTM AGJQPZS**

- Thwarts vanilla frequency analysis

Cryptanalysis of Vigenère

Suppose we know keyword length

- Group letters into **n** buckets, each bucket encrypted using the same shift
- Perform frequency analysis on each bucket

Suppose we don't know keyword length

- Brute force: try several lengths until we get the right one
- Improvement: Kasiski examination, superposition

Kasiski Examination

Published 1863, apparently known to Babbage as early as 1840's

Example:

key: `cryptocryptocryptocryptocryptocryptocrypto`

ptxt: `acannercancanasmanycansasacannercancancans`

ctxt: `CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG`

All **RED**/**PURPLE** chunks are multiples of **6** apart

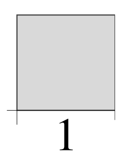
- Good indication that the key length is **1,2,3**, or **6**

Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 1

```
CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
 CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
```

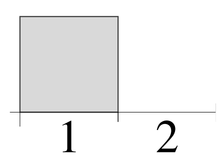


Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 2

```
CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
  CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
```

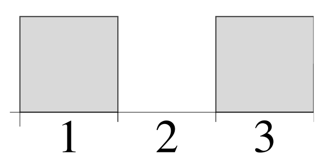


Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example:shift by 3

CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
**   CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG**



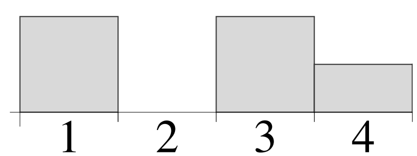
Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 4

CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG

CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG

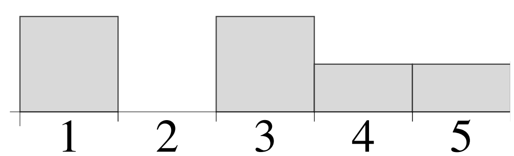


Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 5

```
CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
     CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
```



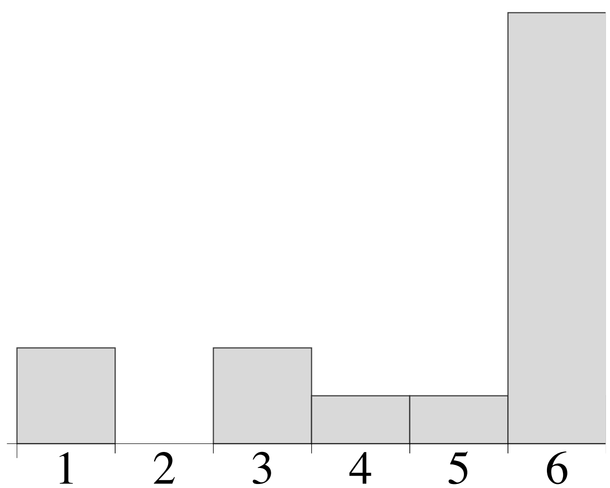
Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 6

CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG

**   CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG**

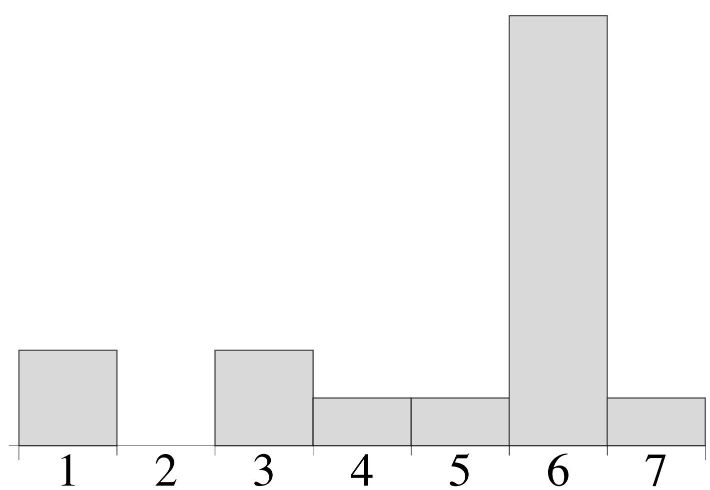


Superposition

Compare shifts of ciphertext, looking for shifts containing many matches

Example: shift by 7

```
CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
       CTYCGSTTYCVOPRQBTBATYCLOURAPGBGIAPGQCEAPGG
```



Superposition

Why does it work?

For shifts that are multiples of key size:

- Both bottom and top ciphertexts encrypted with same key
- **#(ctxt matches) = #(ptxt matches)**
  ≈ |ptxt| * col. prob. for English
  ≈ |ptxt| * 0.065

Superposition

Why does it work?

For shifts that are NOT multiplies of key size:

- Both bottom and top ciphertexts encrypted with "independent" shifts
- Probability of a match at any position is **1/26 ≈ 0.038**
- **#(ctxt matches) ≈ |ptxt| * 0.038**

Disk-based Substitution Ciphers

First Invented by Alberti, 1467

*

†

‡

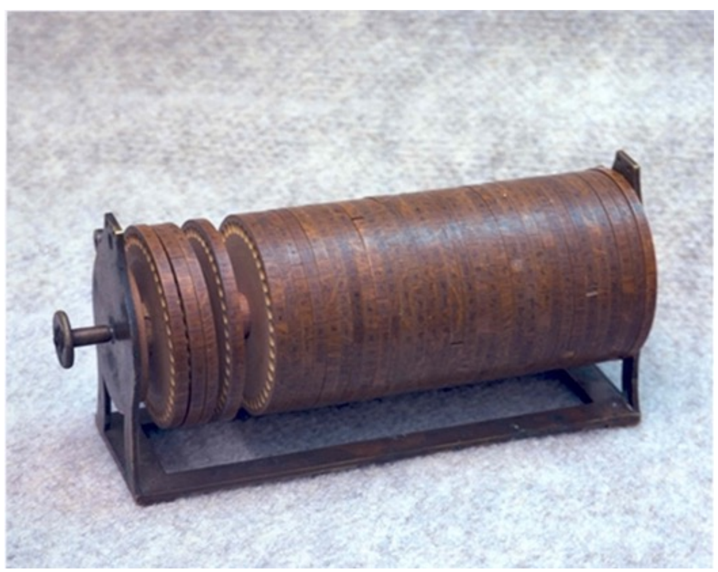
* cropped from http://www.cryptomuseum.com/crypto/usa/ccd/img/301058/000/full.jpg
† cropped from https://www.flickr.com/photos/austinmills/13430514/sizes/l
‡ https://commons.wikimedia.org/wiki/File:Captain-midnight-decoder.jpg

Disk-based Substitution Ciphers

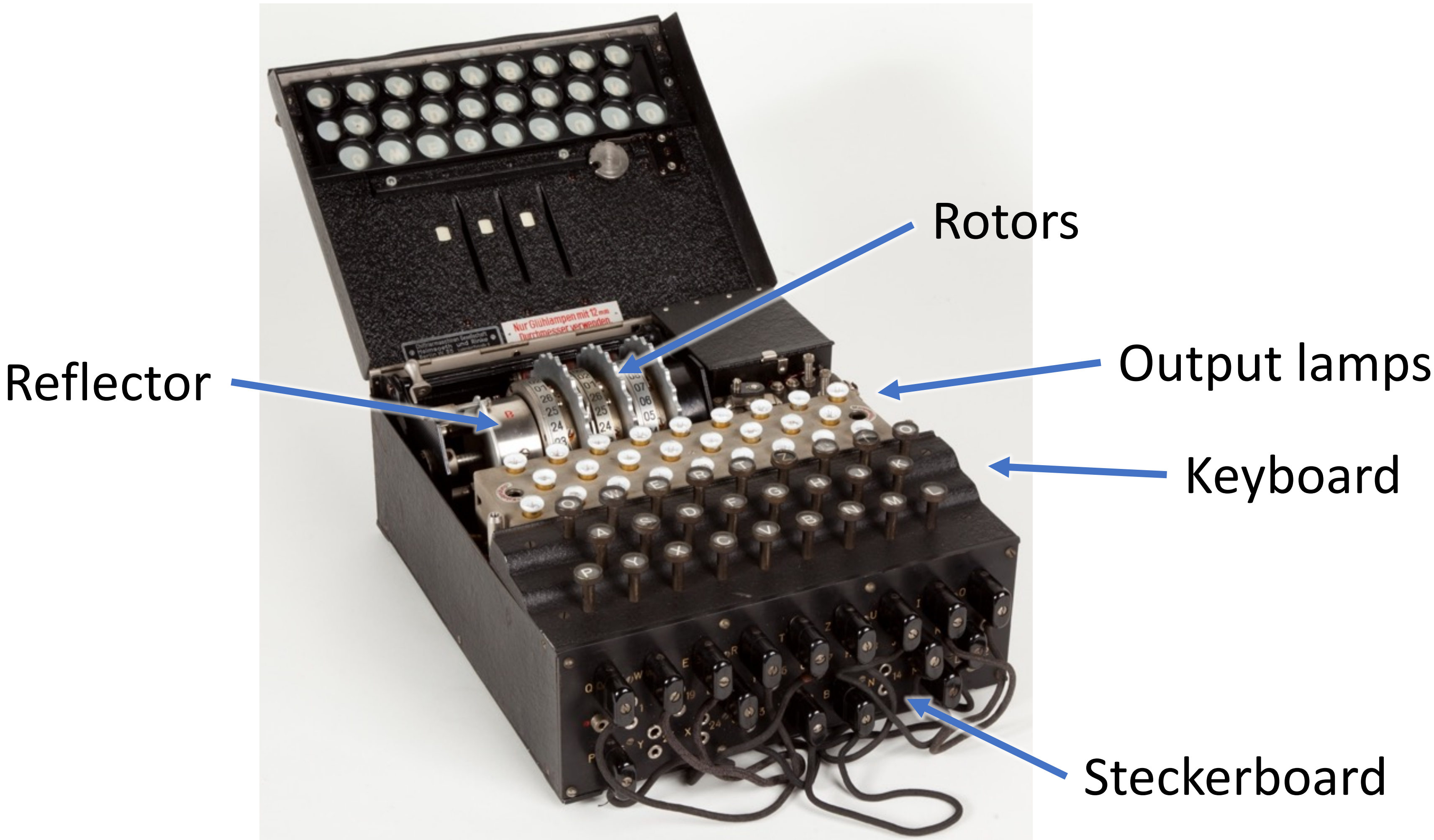
In most basic form, simple monoalphabetic cipher

Alberti Cipher – rotate the disk periodically
- Considered the first polyalphebetic cipher

Jefferson disk: used by US military until WWII

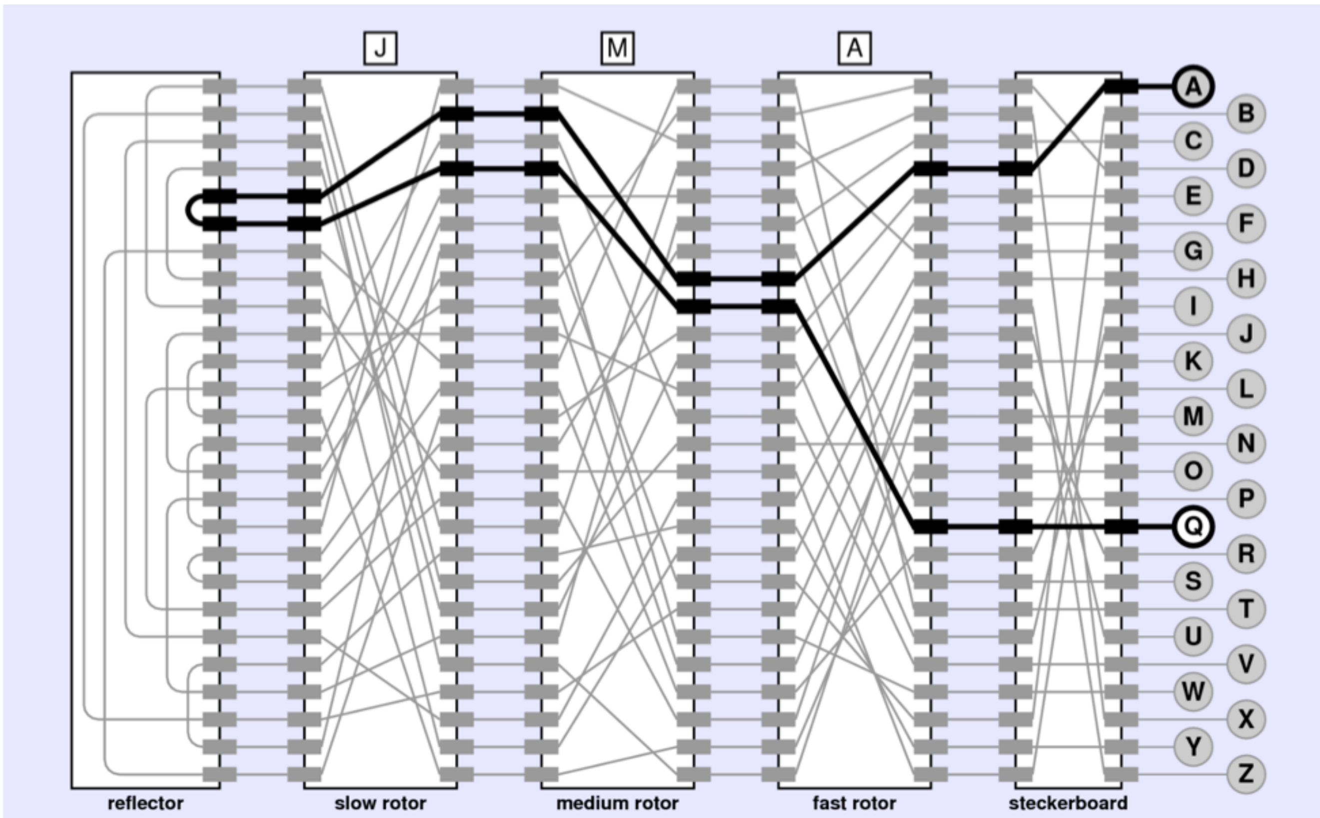


The German Enigma Machine



https://commons.wikimedia.org/wiki/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

Enigma Diagram



http://stanford.edu/class/archive/cs/cs106a/cs106a.1164/handouts/29A-CryptographyChapter.pdf

- With each key stroke, fast rotor rotates by 1
- Each time fast rotor completes a revolution, medium rotor rotates by 1
- Each time medium rotor completes a revolution, slow rotor rotates by 1

Enigma Keys

Key:

- Selection of 3 rotors out of 5 (60 possibilities)
- Initial rotor setting (26^3)
- Steckerboard wiring (216,751,064,975,576)

Possible attack strategies?

- Brute force
  - 2^{68} possible keys: feasible today, but not in WWII
- Frequency analysis
  - Polyalphabetic with key length $26^3 = 17576$
  - Likely no key was used to encrypt enough material

Cracking the Enigma

First developed in Poland, improved by Blechtley Park

<u>User error/bad practices</u>

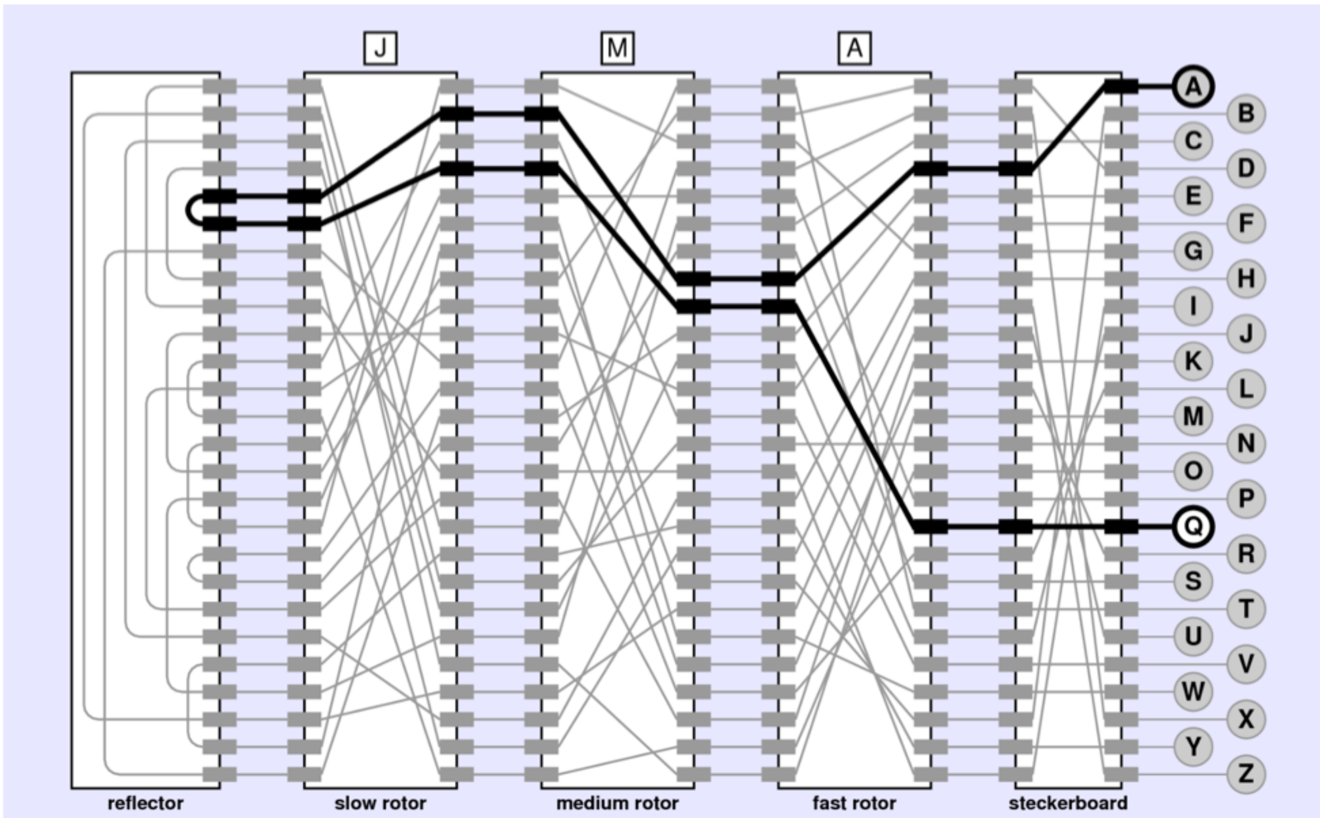
<u>Known plaintext attack</u>

- Often possible to predict part of plaintext

<u>Structural features</u>

- Symmetry
- Cannot map a character to itself
- Steckerboard applies fixed permutation on both ends

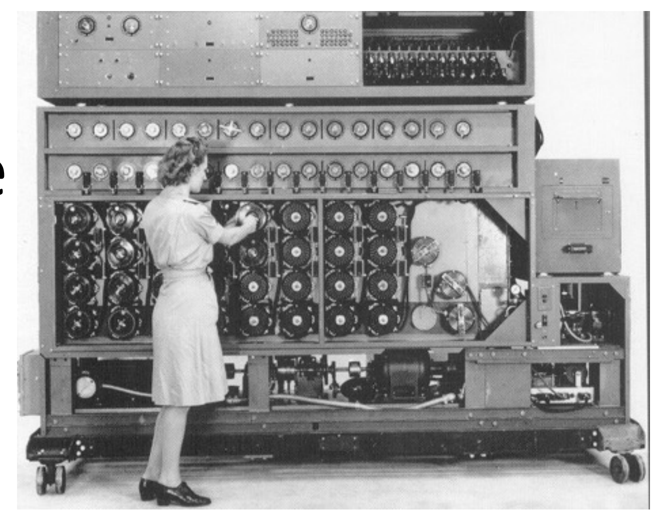
Enigma Diagram



http://stanford.edu/class/archive/cs/cs106a/cs106a.1164/handouts/29A-CryptographyChapter.pdf

A Key Insight: Loops

- Loops unaffected by steckerboard wiring
- Only need to search the $\approx 2^{20}$ rotor positions to find one that generates such a loop
- Possible at the time using the Bombe



http://www.cryptomuseum.com/crypto/bombe/img/us_bombe_full.jpg

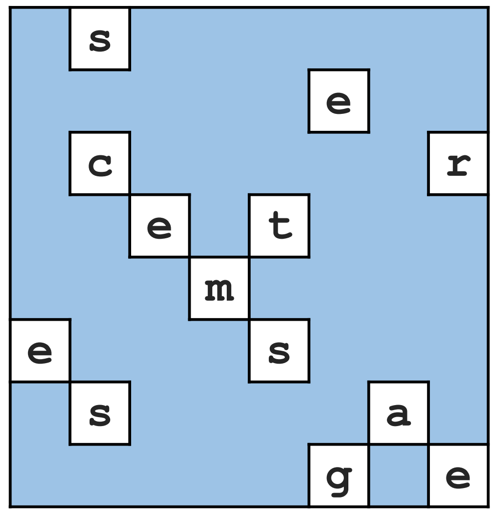
Switching Gears: Transposition Ciphers

Shuffle plaintext characters

Greek Scytal (600’s B.C.)

https://commons.wikimedia.org/wiki/File:Skytale.png

Grille (1500’s A.D.)



a	s	h	o	e	v	q	k
g	i	p	c	e	e	f	j
e	c	n	i	d	z	w	r
g	i	e	b	t	e	b	o
k	c	d	m	i	z	d	p
e	b	i	d	s	h	e	r
n	s	d	u	r	e	a	v
h	k	e	g	u	g	a	e

Column Transposition

key: **crypto**

ptxt: **supersecremessage**

Encryption:

c	r	y	p	t	o
s	u	p	e	r	s
e	c	r	e	t	m
e	s	s	a	g	e

Sort by first row →

c	o	p	r	t	y
s	s	e	u	r	p
e	m	e	c	t	r
e	e	a	s	g	s

ctxt: **SEESMEEEEAUCSRTGPRS** (read off columns)

Cryptanalysis:

- Guess key length, reconstruct table
- Look for anagrams in the rows

Double Column Transposition

key: **graphy**

ctxt0: **SEESMEEEAUCSRTGPRS**

Encryption:

g	r	a	p	h	y
s	e	e	s	m	e
e	e	a	u	c	s
r	t	g	p	r	s

Sort by first row →

a	g	h	p	r	y
e	s	m	s	e	e
a	e	c	u	e	s
g	r	r	p	t	s

ctxt: **EAGSERMCRSUPEETESS**

Example: Germany, WWI

- French were able to decrypt after seeing several messages of the same length

Anagrams and Astronomy

<u>Galileo and the Rings of Saturn</u>

- Galileo observed the rings of Saturn, but mistook them for two moons

- Galileo wanted extra time for verification, but not to get scooped
- Circulates anagram
  SMAISMRMILMEPOETALEUMIBUNENUGTTAUIRAS
- When ready, tell everyone the solution:
  altissimum planetam tergeminum observavi
  (“I have observed the highest planet tri-form”)

Anagrams and Astronomy

<u>Enter Huygens</u>

- Realizes Galileo actually saw rings
- Circulates

AAAAAAA CCCCC D EEEEE G H IIIIIII LLLL MM NNNNNNNNN OOOO PP Q RR S TTTTT UUUUU

- Solution:

annulo cingitur, tenui, plano, nusquam cohaerente, ad eclipticam inclinato

(“it is surrounded by a thin flat ring, nowhere touching, and inclined to the ecliptic”)

Commitment Scheme

Different than encryption

- No need for a decryption procedure
- No secret key
- But still need secrecy ("hiding")
- Should only be one possible opening ("binding")
- Sometimes other properties needed as well…

Anagrams are Bad Commitments

If too short (e.g. one, two, three words), possible to reconstruct answer

If too long, multiple possible solutions

- Kepler tries to solve Galileo's anagram as

`salue umbistineum geminatum martia proles`

(hail, twin companionship, children of Mars)

Anagrams are Bad Commitments

Huygens Discovers Saturn's moon Titan

- Sends the following to Wallis

`ADMOVERE OCULIS DISTANTIA SIDERA NOSTRIS, UUUUUUUCCCRR-HNBQX`

(First part meaning "to direct our eyes to distant stars")

Plaintext: **`saturno luna sua circunducitur diebus sexdecim horis quatuor`**

("Saturn's moon is led around it in sixteen days and four hours")

Anagrams are Bad Commitments

<u>Huygens Discovers Saturn’s moon Titan</u>

- Wallis replies with

AAAAAAAAA B CCCCC DDDD EEEEEEEEE F H
IIIIIIIIIIII LLL MMMMMM NNNNNN OOOOOOO PPPPP
Q RRRRRRRRRRR SSSSSSSSSSSSS TTTTTTTT
UUUUUUUUUUUUUUUUU X

(Contains all of the letters in Huygens’ message, plus some)

Anagrams are Bad Commitments

Huygens Discovers Saturn's moon Titan

- When Huygens finally reveals his discovery, Wallis responds by giving solution to his anagram:

saturni comes quasi lunando vehitur. diebus sexdecim circuitu rotatur. novas nuper saturni formas telescopo vidimus primitus. plura speramus

("A companion of Saturn is carried in a curve. It is turned by a revolution in sixteen days. We have recently observed new shapes of Saturn with a telescope. We expect more.")

- Tricked Huygens into thinking British astronomers had already discovered Titan

Lessons

Transposition ciphers should not be considered secure

Substitution ciphers should not be considered secure **unless** polyalphabetic where key has very long period

But, using both together can provide reasonable security if done correctly

- Substitution permutation networks

Bifid Cipher

Polybius square + Transposition + Inverse Polybius

	1	2	3	4	5
1	y	n	r	b	f
2	d	l	w	o	g
3	s	p	a	t	k
4	h	v	ij	x	c
5	q	u	z	e	m

plaintext: **super secret message**

Polybius: **35351 354153 5533325**
12243 145344 5411354

Transpose: **353513541535533325122431453445411354**

Inv.Polybius: **k k r e f k z a g n o s c t c h r e**

Bifid Cipher

Polybius square + Transposition + Inverse Polybius

Invented in 1901 by Felix Delastelle

Each ctxt character depends on **two** ptxt characters

- Still possible to break using frequency analysis

Repetition?

- Double Bifid: each ctxt char depends on **four** ptxt chars
- Triple Bifid: each ctxt char depends on **eight** ptxt chars
- ...

Bifid Cipher

Polybius square + Transposition + Inverse Polybius

Invented in 1901 by Felix Delastelle

Each ctxt character depends on **two** ptxt characters

- Still possible to break using frequency analysis

Repetition?

- D… hars
- Tr… ars
- …

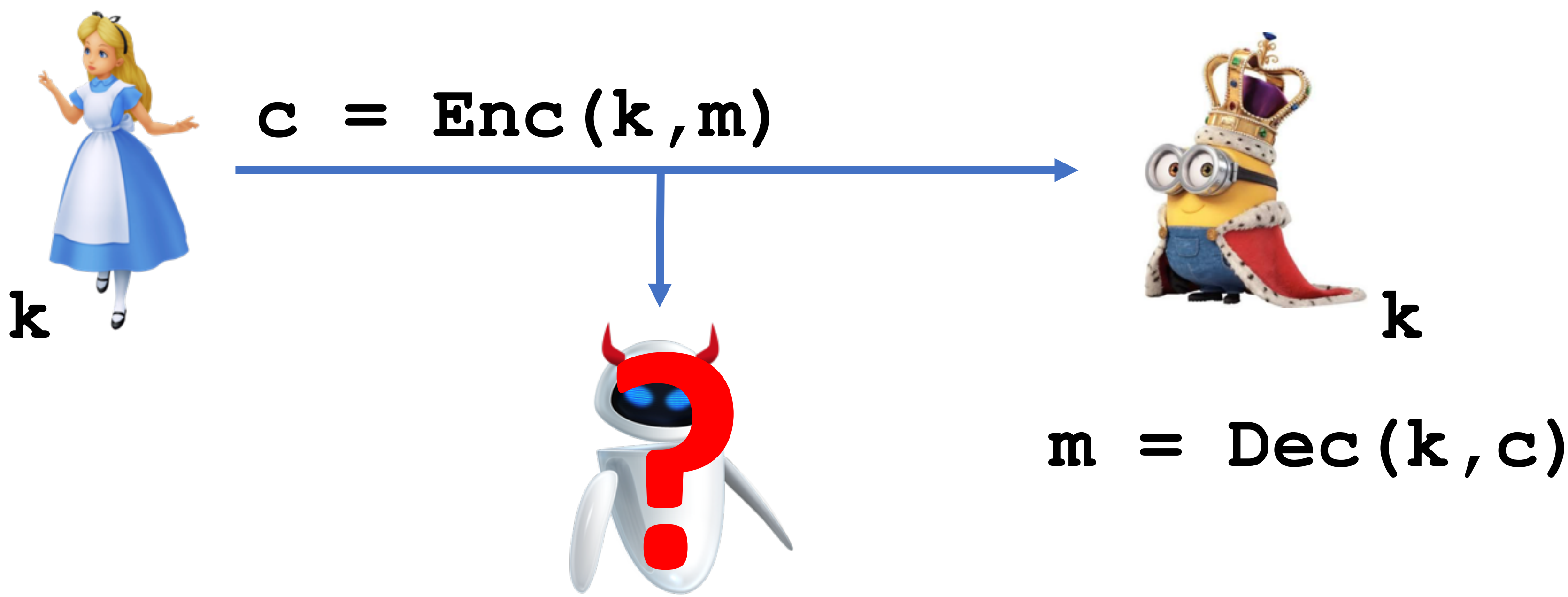
Modern ciphers ensure that every ctxt character depends on every ptxt character (necessary but not sufficient for security)

Modern Cryptography

Mid 1970’s – Present

Several key advancements

- Asymmetric (public key) cryptography

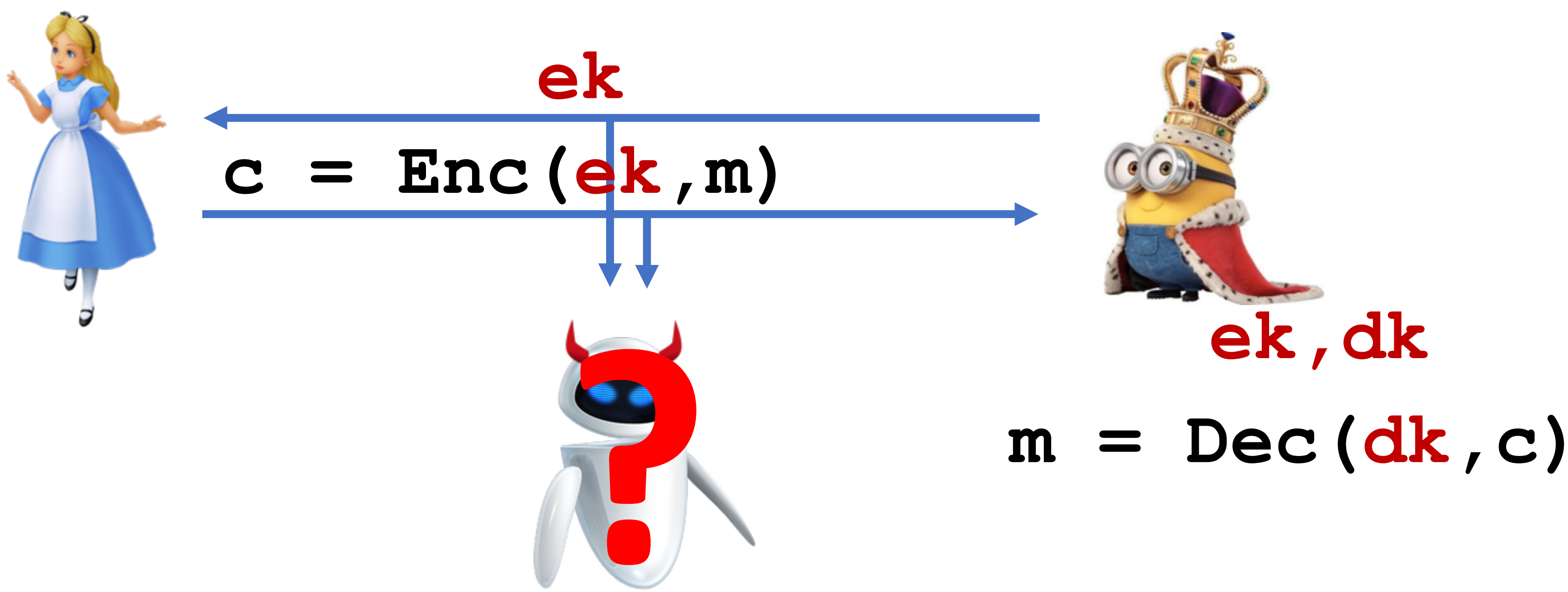


Modern Cryptography

Mid 1970's – Present

Several key advancements

- Asymmetric (public key) cryptography



Modern Cryptography

Mid 1970's – Present

Several key advancements

- Asymmetric (public key) cryptography
- Beyond secrecy
  - Authentication, integrity, commitments, etc
- Rigorous definitions
  - Encrypt same message twice? Part of the message known?
- Formal proofs of security *

* In most cases, some assumptions need to be made

Modern Cryptography

Mid 1970's – Present

Several key advancements

Breaking crypto itself is no longer considered top cybersecurity threat

- Most hacks are the result of system vulnerabilities, social engineering, poor use of cryptography

Starting next time: mathematical ideas behind modern cryptosystems

Next Time

Defining encryption

The one-time pad

Remember: enroll on Piazza