601.445/645
Practical Cryptographic Systems

Symmetric Cryptography

Instructor: Matthew Green

Piazza

- We will use Piazza for all communications, including schedule changes and snow days
- You must sign up!
- You can also find links to all of the class resources (syllabus, readings, Gradescope, etc.)

https://piazza.com/jhu/spring2025/601445601645

Housekeeping

- Waitlist: I promise that if you stick it out you will get into the class
- **Assignment 1: out last Friday! (Check Piazza!)**
  - This is a written+programming assignment in classical cryptography with a hint of statistics
  - Should also appear on the “Assignments” page in our Git repo

    https://github.com/matthewdgreen/practicalcrypto
- **TA office hours: 5:30-6:30 Mondays, Malone 216**

News

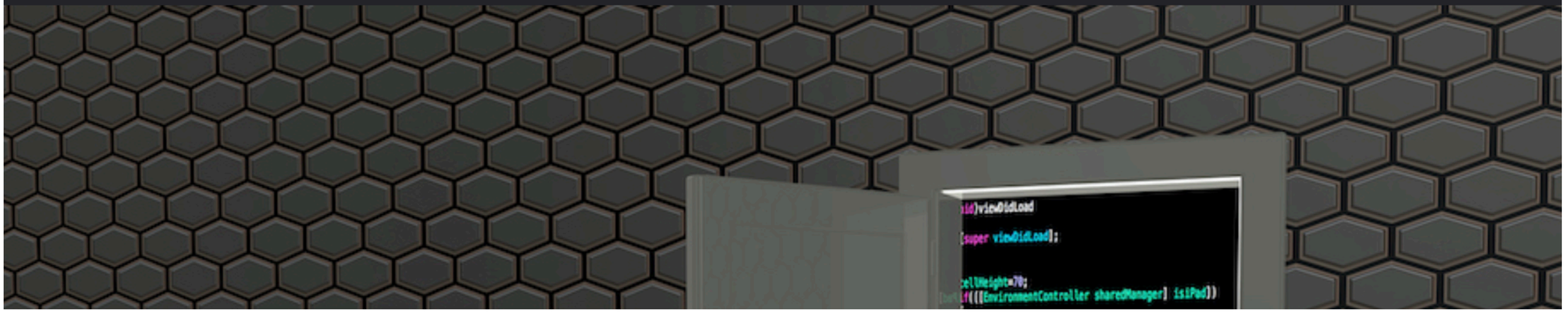
ars TECHNICA SECTIONS FORUM SIG

A "COMPLETELY INVISIBLE" BACKDOOR

Backdoor infecting VPNs used “magic packets” for stealth and security

J-Magic backdoor infected organizations in a wide array of industries.

DAN GOODIN – JAN 23, 2025 6:42 PM | 35



News

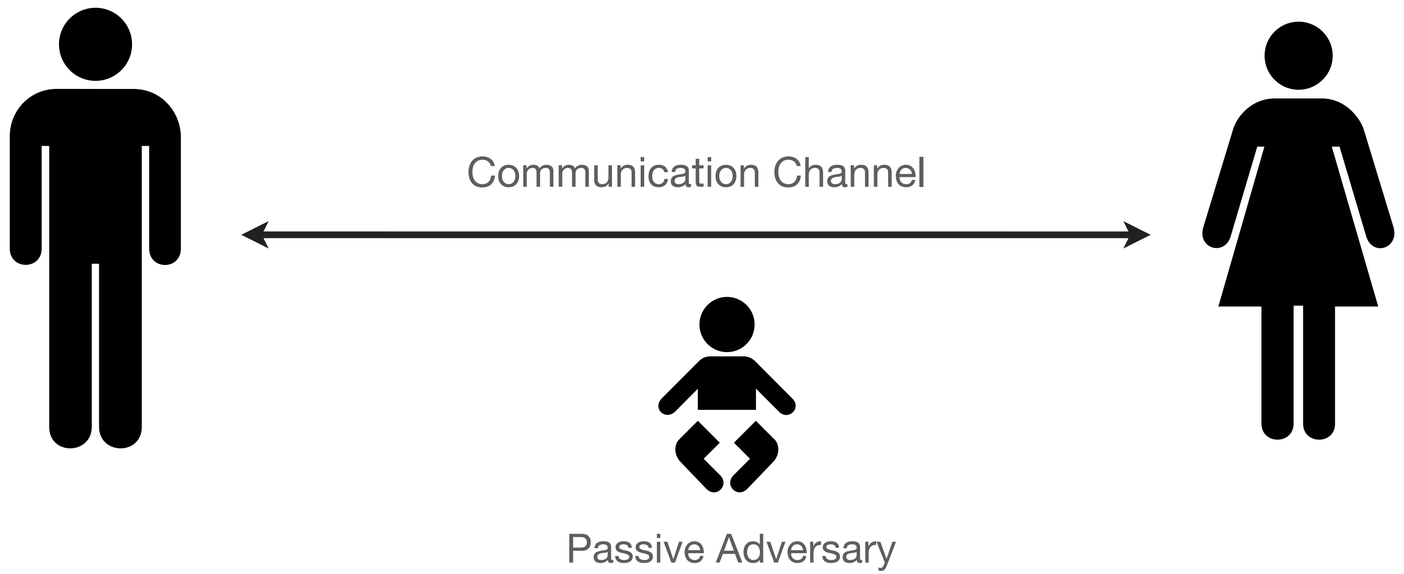
J-Magic, the tracking name for the backdoor, goes one step further to prevent unauthorized access. After receiving a magic packet hidden in the normal flow of TCP traffic, it relays a challenge to the device that sent it. The challenge comes in the form of a string of text that’s encrypted using the public portion of an RSA key. The initiating party must then respond with the corresponding plaintext, proving it has access to the secret key.

Review

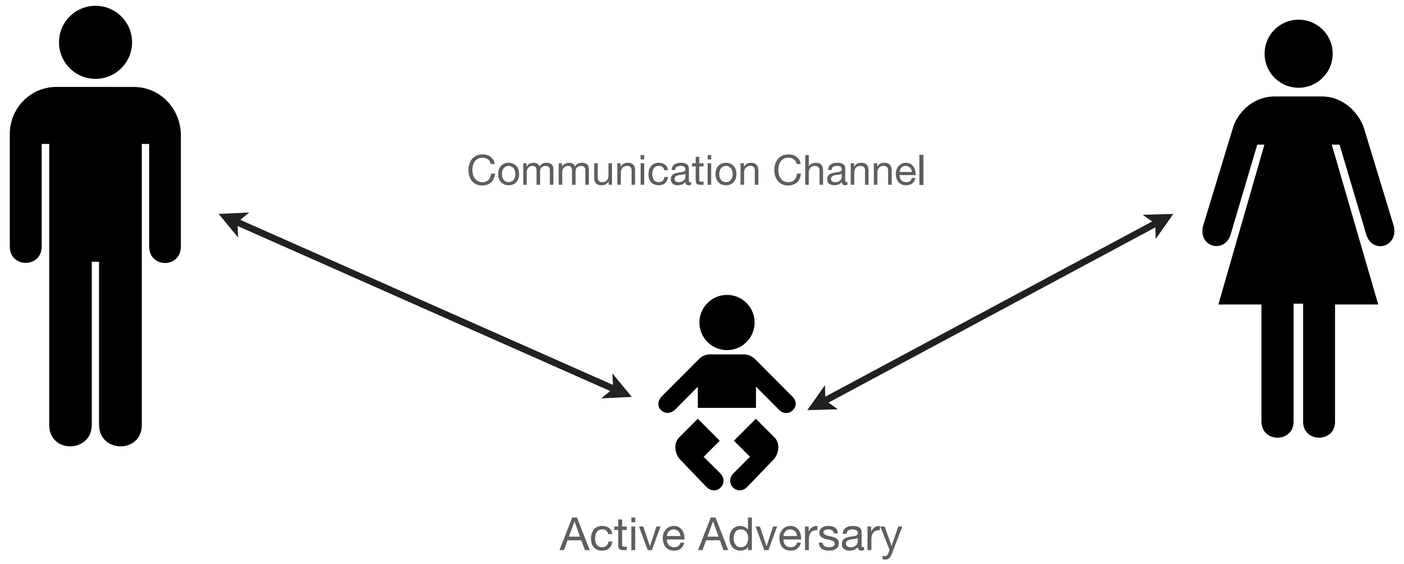
- Last time:
  - A few examples of how systems break
  - Bad primitives, bad protocols, bad implementation
- Today & Weds:
  - A (brief) tour through cryptologic history
  - Starting with symmetric (secret-key) crypto

Communication Model

Communication Model



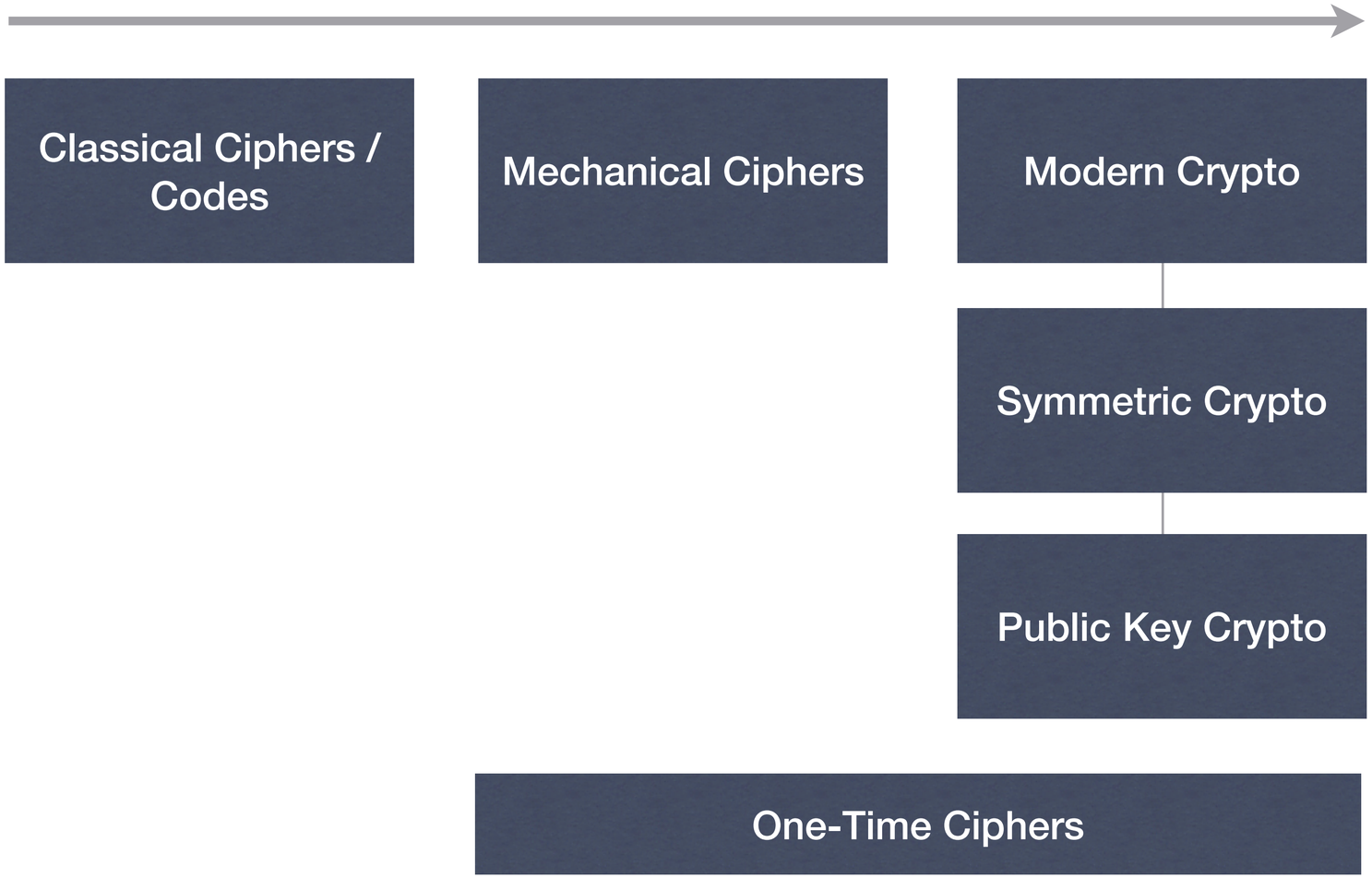
Communication Model



Secure Communication

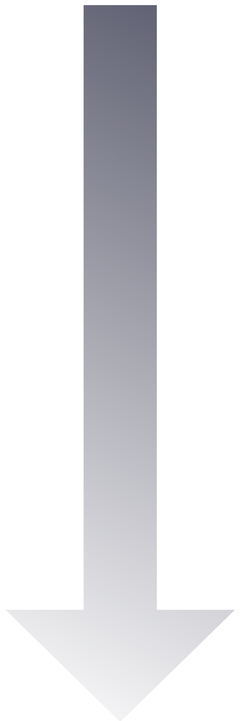
- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)
- Tools:
  - Encryption
  - Message Authentication Codes (MACs)
  - Digital Signatures

History of Encryption



Classical Cryptography

- Beginning of time to 1900s or so
  - Shift (Caesar) cipher
  - Substitution ciphers
  - Polyalphabetic ciphers (Vigenère)
  - Digraph ciphers (Playfair)
  - A multitude of others...



Increasing Complexity

<- Load New Puzzle

Tractability:11655

CRYPTOGRAM

Points 979

4/1/2009 0:21

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

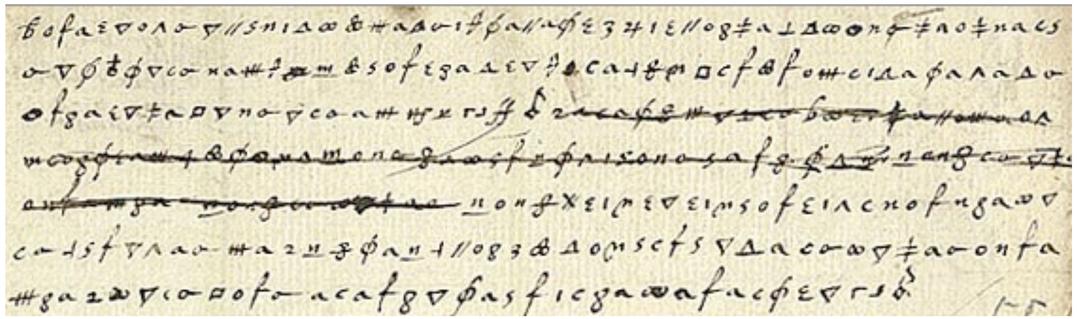
' P I G C G M N N U J C Y L I P G T Y T L P I Y T L M S F E P

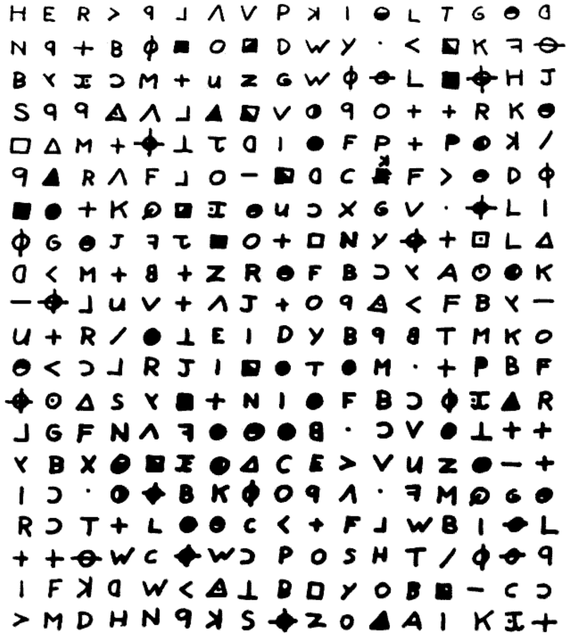
'

V Y K K N G M L G Y H P I M P U F E R T F O U F E ' N N L C F O

F E P F J Y P . ' - K F C Y H K M U

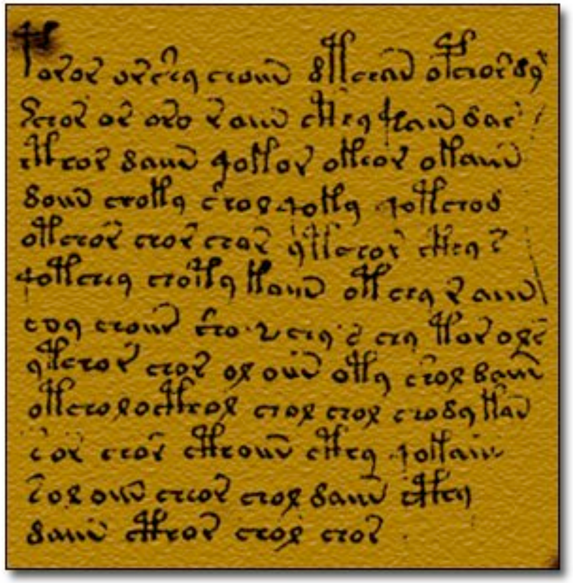
. ' -





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

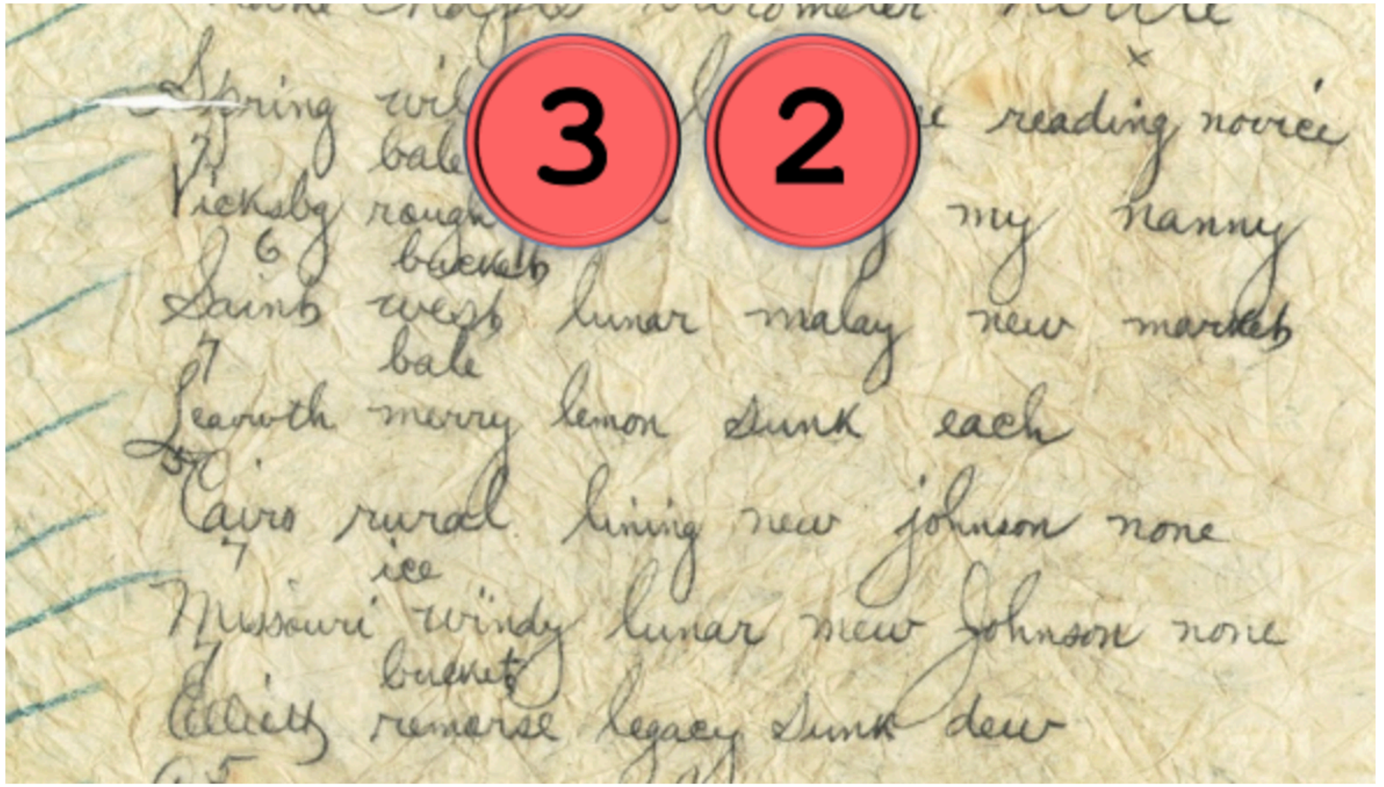
S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A




78

The Top 50 unsolved encrypted messages: 32. The silk dress cryptogram

Von Klaus Schmeh / 13. Mai 2017 / 6 Kommentare / Seite 1 von 2 / Auf einer Seite lesen



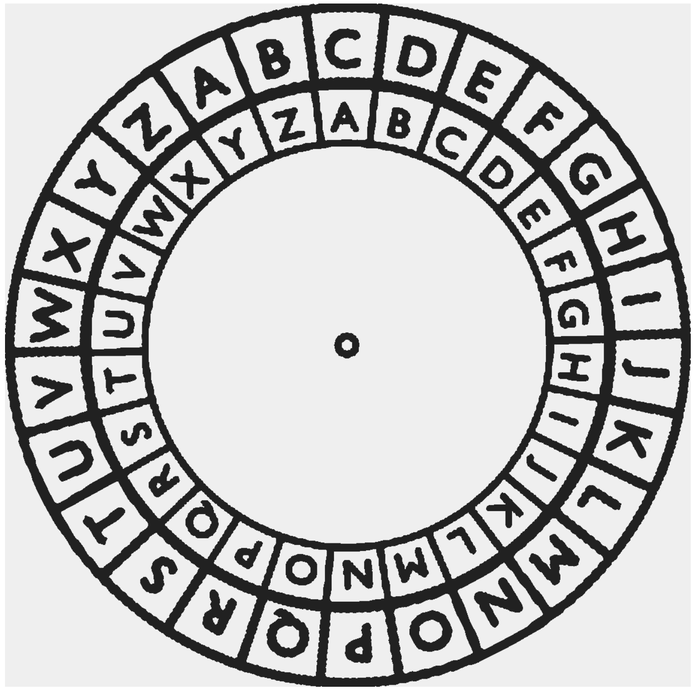
Shift (“Caesar”) cipher

- Key is a “shift value” (0 through 25)
- We take a plaintext and “shift” each letter through the alphabet:

  Example, key = 10.

  A T T A C K

  K D D K M U



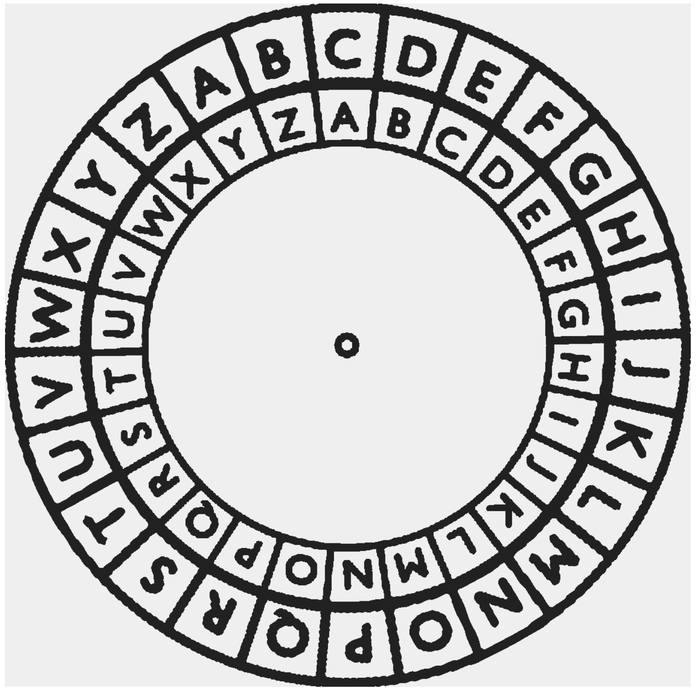
Shift (“Caesar”) cipher

- Key is a “shift value” (0 through 25)
- We take a plaintext and “shift” each letter through the alphabet:

  Example, key = 10.

  A T T A C K

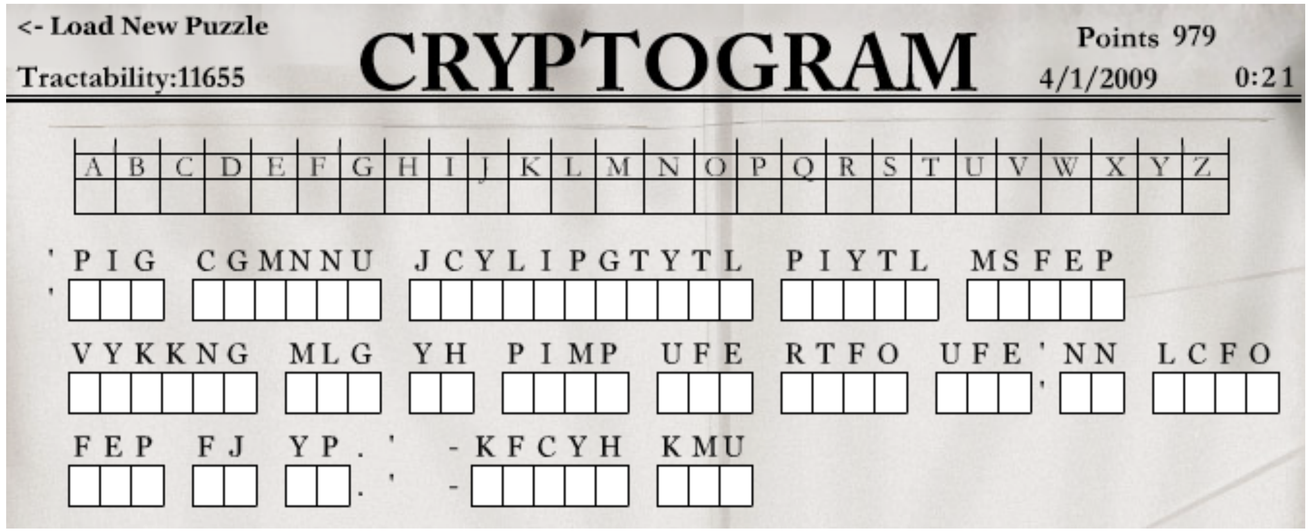
  K D D K M U



Limitations of the shift cipher?

Substitution cipher

- Shift cipher has a small *key space*
  - This means it is vulnerable to “brute force attack”
- *We need a cipher with a larger set of possible keys*
- One solution is the substitution cipher



How many keys in an (alphabetic) substitution cipher?

How many keys in an (alphabetic) substitution cipher?

Figure 2.1: Example key for a simple substitution cipher.

How many keys in an (alphabetic) substitution cipher?

Figure 2.1: Example key for a simple substitution cipher.

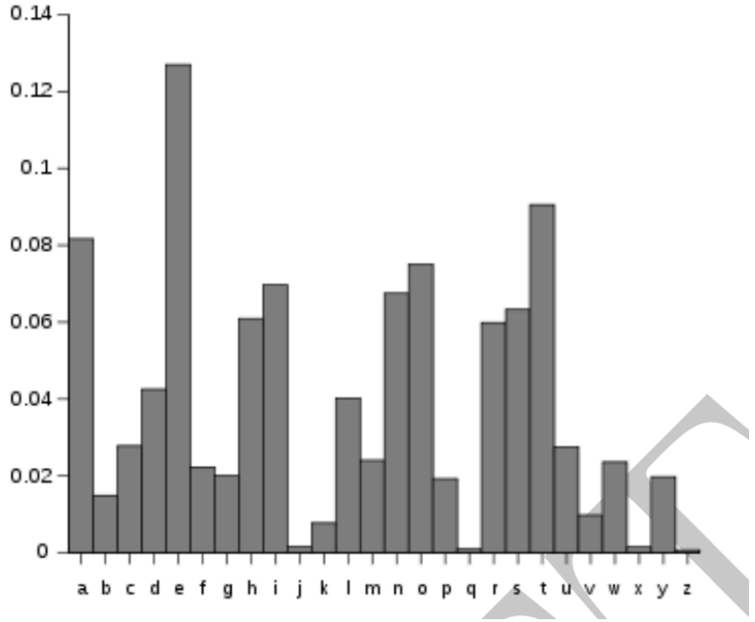
#keys = 26 * 25 * 24 * … * 2 * 1

= 26! = 403 *trillion trillion* = about 2^88

So what’s wrong with substitution ciphers?

So what's wrong with substitution ciphers?

- Many things:
  - They leak letter patterns (e.g., repeated letters)
  - They leak letter frequency
- This is because the substitution "key" is the same for every letter



Vigenere

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One-Time Ciphers

- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher

•Based on Baudot code for Teletypes

•Added (XORed) a random Key (sequence of bits) to a binary message

- Perfectly secure, provided:

•key is perfectly random

•key is at least as long as the message

•key is never re-used

(No Model.)

11 Sheets—Sheet 6.

J. M. E. BAUDOT.

PRINTING TELEGRAPH.

No. 388,244. Patented Aug. 21, 1888.

Fig. 24.

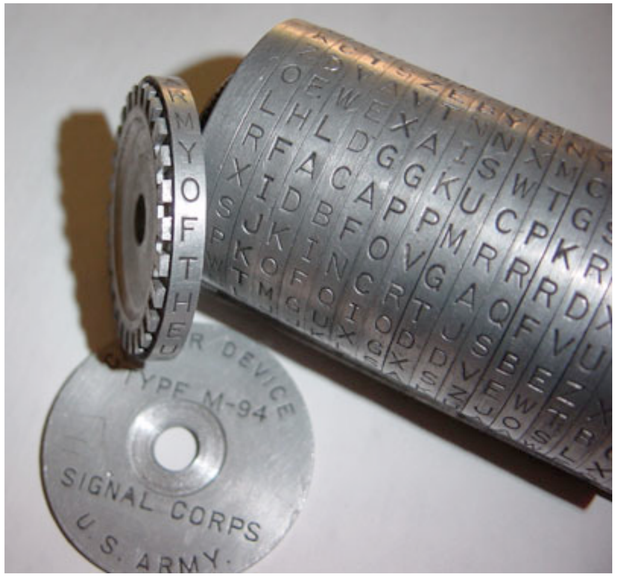
	1	2	3	4	5
A	+	−	−	−	−
B	−	−	+	+	−
C	+	−	+	+	−
D	+	+	+	−	−
E	−	+	−	−	−
F	+	+	−	+	−
G	−	+	−	+	−
H	+	+	−	+	−
I	−	−	+	−	−
J	+	−	+	−	−
K	+	+	+	−	+
L	−	+	+	+	+
M	+	+	+	+	+
N	−	+	+	+	−
O	+	+	+	+	+
P	+	−	+	+	+
Q	−	−	+	−	+
R	−	−	+	−	+
S	+	−	+	−	−
T	−	−	+	−	+
U	+	+	+	−	+
V	−	+	−	−	+
W	−	+	−	−	+
X	+	−	+	−	−
Y	+	−	−	−	+
Z	−	−	−	+	+
Ł	−	−	−	+	−
Ń	−	−	−	−	+

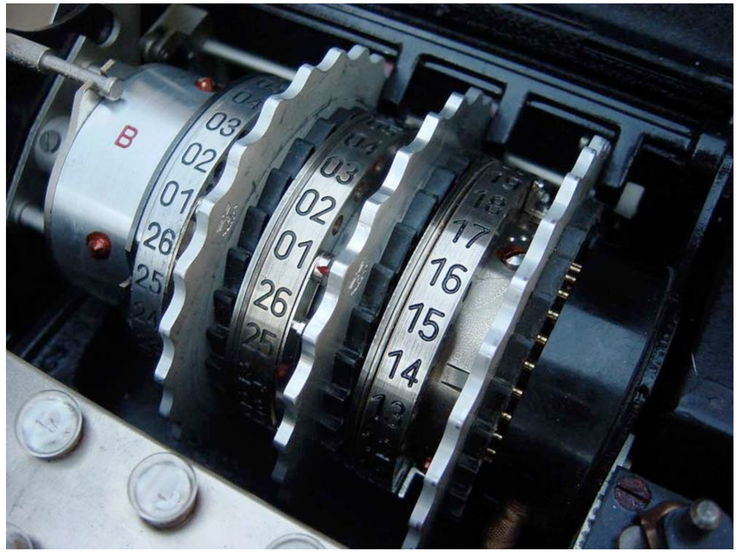
INVENTOR:

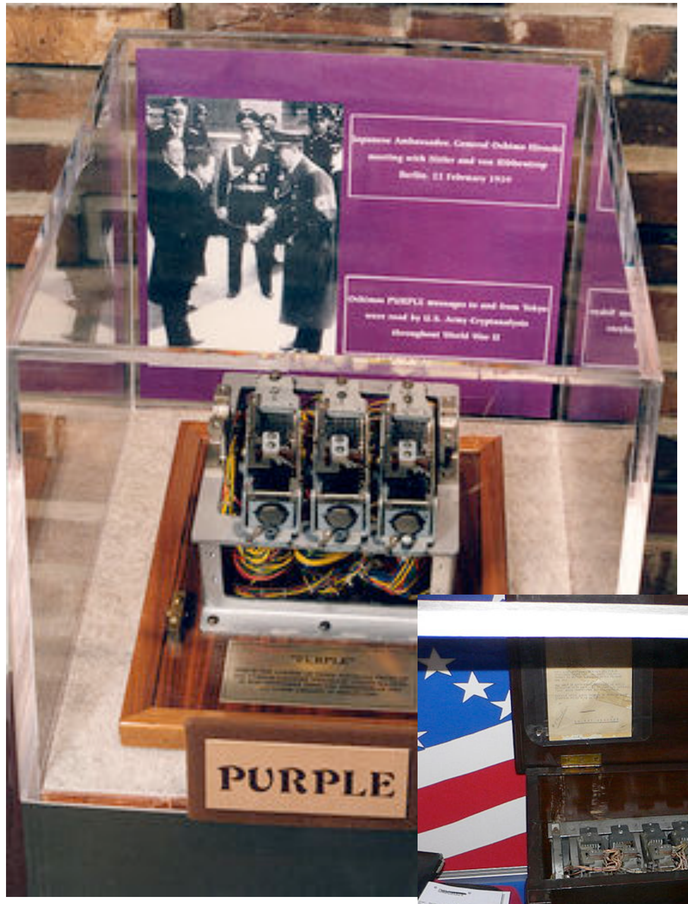
Jean Maurice Émile Baudot

Mechanical Cryptography

- 1900s
  - Mass production and usage of cipher devices
  - Rotor ciphers
  - Electronic devices







HAGELIN M-209 CIPHER MACHINE (GVG / PD)


0015
AB CD EF GH I J KL MN OP QR ST UV WX YZ
AB CD EF GH I J KL MN OP QR ST UV WX YZ
0 AB
1 CD
2 EF
3 GH
4 I J
5 KL
6 MN
7 OP
8 ST
9 UV