CS 100: Encryption and Passwords

Chris Kauffman

Week 8-2

Logistics

Feedback

- Midterm overall scores on Blackboard
- Advisory Grades to be posted tomorrow
- Feedback from you today

Today

- Encryption
- Password Selection
- The internet

HW 4 Due Tonight

HW 5 Up Friday

- Will post this weekend
- Simple Encryption Problems
- Creating your own personal web page

Reading: Pattern Ch 6

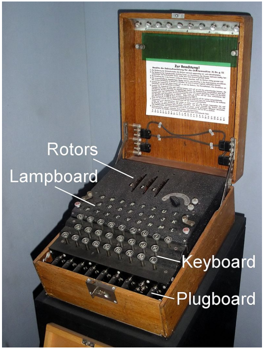
Pre-computer Encryption

Encryption is based on a combination of two principles

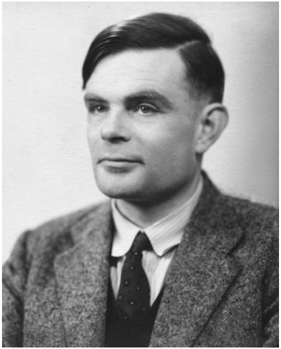
1. Don't know the encryption process (obscurity)
2. Don't know some necessary secret that helps decrypt (strength)

Historically it was super hard to do, based more on (1)

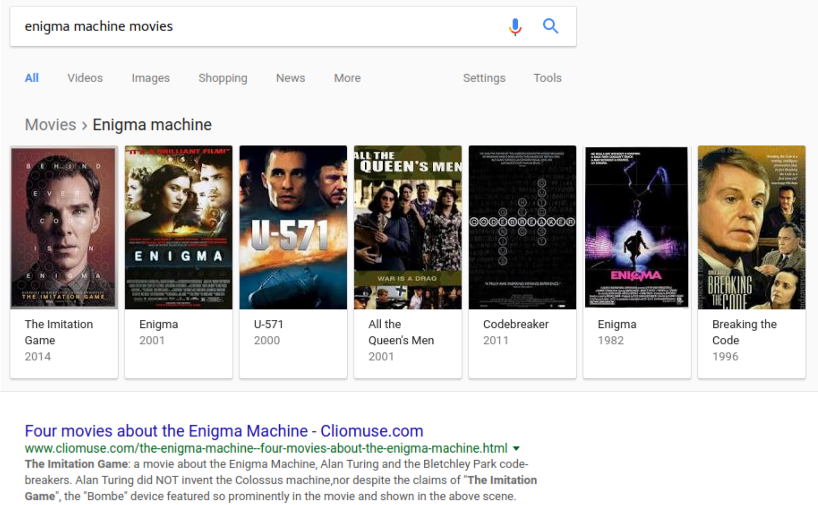
German Enigma Machine



Alan Turing



Enigma features prominently in Film



enigma machine movies

All Videos Images Shopping News More Settings Tools

Movies › Enigma machine

The Imitation Game
2014

Enigma
2001

U-571
2000

All the Queen's Men
2001

Codebreaker
2011

Enigma
1982

Breaking the Code
1996

Four movies about the Enigma Machine - Cliomuse.com
www.cliomuse.com/the-enigma-machine--four-movies-about-the-enigma-machine.html ▾
The Imitation Game: a movie about the Enigma Machine, Alan Turing and the Bletchley Park code-breakers. Alan Turing did NOT invent the Colossus machine,nor despite the claims of "**The Imitation Game**", the "Bombe" device featured so prominently in the movie and shown in the above scene.

Encryption

- Obscure information except for the intended recipient
- Usually involves a shared secret
- Caesar Cipher
  - Constant shift of characters
  - Secret key is the `shift` amount
  - Not very strong encryption
- Vigenere Cipher
  - Variable shift of characters
  - Secret key is the pass phrase
- A good video on Caesar and Vigenere Ciphers for beginners

Caesar Cipher Example

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Example 1

Secret Key +4

Plain Text `MARIO`

Encrypted `QEVMS`

Work It

Secret Key +9

Encrypted `CXJM`

Plain Text `????`

Example 2

Secret Key +7

Plain Text `LUIGI`

Encrypted `SBPNP`

Notice the wrapping of `U`

- U→ 21;
- (20+7) % 26 = 27 % 26 = 1
- 1 → `B`

Vigenere Cipher

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Don't use a single key, use a passphrase

Secret Key `TOAD` → `[19, 14, 0, 3]`

Plain Text `PRINCESS`

Encrypted `IFJQVSSV`

Original	P	R	I	N	C	E	S	S
Numbers	15	17	8	13	2	4	18	18
Secret Key	T	O	A	D	T	O	A	D
Numbers	19	14	0	3	19	14	0	3
Sums	34	31	8	16	21	18	18	21
modulo 26	8	5	I	16	21	18	18	21
Encrypted	I	F	J	Q	V	S	S	V

Exercise: Decrypt, Encrypt

0	1	2	3	4	5	6	7	8	9	10	11	12	
A	B	C	D	E	F	G	H	I	J	K	L	M	
13	14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_

Caeasar Cipher

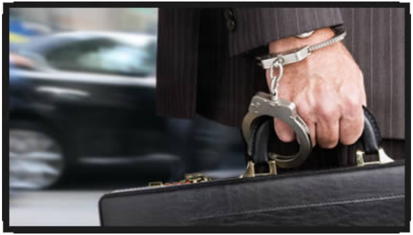
- Secret Key: 4
- Encrypted Text `GWDJYR`
- Plain Text: ???

Vigenere

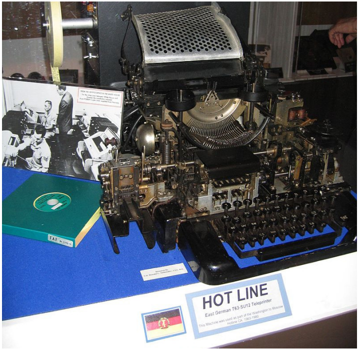
- Secret Key: `KEY`
- Plain Text: `ENCRYPT`
- Encrypted Text: ???

Cold War Crypto

- Sharing an encryption key was hard work
- Send somebody in person with the key on paper/disk
- Make sure they get it there without anyone sawing their arm off



During the [Cuban Missile] crisis, it took the United States nearly twelve hours to receive and decode Nikita Khrushchev's 3,000-word initial settlement message - a dangerously long time in the chronology of nuclear brinkmanship. Wiki:Hotline


HOT LINE
East German T63-SU12 Teleprinter
This Machine was used as part of the Washington to Moscow Hotline CA. 1963-1980

Exercise: Summarize Basic Encryption

- How does the Caesar Cipher work?
- What form of secret is required in the Caesar Cipher and who has to know it?
- What is the Vigenere Cipher?
- What form of secret is required in Vigenere and who has to know it?

Breaking Encryption

0	1	2	3	4	5	6	7	8	9	10	11	12	
A	B	C	D	E	F	G	H	I	J	K	L	M	
13	14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_

Mario to Luigi: *I need this for personal growth!*

Message:

W	D	B	R	A	Y	Y	W
22	3	1	17	0	24	24	22

Think like a Hacker

- Want to know the contents of message but don't know the encryption key
- How can the encryption key be found?
  Hint: guess and check
- How long will this take

Write A Loop

```
for i in range(28):
  print(str(i)+" "+caesar_decrypt(encrypted, i))
```

```
 0 WDBRAYYW
 1 VCAQ_XXV
 2 UB_PZWWU
 3 TAZOYVVT
 4 S_YNXUUS
 5 RZXMWTTR
 6 QYWLVSSQ
 7 PXVKURRP
 8 OWUJTQQO
 9 NVTISPPN
10 MUSHROOM
11 LTRGQNNL
12 KSQFPMMK
13 JRPEOLLJ
14 IQODNKKI
15 HPNCMJJH
16 GOMBLIIG
17 FNLAKHHF
18 EMK_JGGE
19 DLJZIFFD
20 CKIYHEEC
21 BJHXGDDB
22 AIGWFCCA
23 _HFVEBB_
24 ZGEUDAAZ
25 YFDTC__Y
26 XECSBZZX
27 WDBRAYYW
```

Key Found

Key = 10

	M	U	S	H	R	O	O	M
	12	20	18	7	17	14	14	12
	+10	+10	+10	+10	+10	+10	+10	+10
	22	30	28	17	27	24	24	22
% 27	22	3	1	17	0	24	24	22
	W	A	C	R	B	X	X	W

What does this tell us about the strength of the Caesar Cipher?

Password Storage Uses Encryption

- Secure Hash: 1-way Encryption without a password
- I pick my password

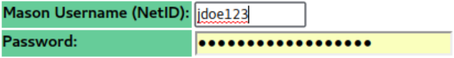
  `kitty123`
- Web Server computes an encrypted, secure hash for the password

  `hash("kitty123") -> 89FA210B6CE92`
- Web server stores username and password

  `jdoe123 : 89FA210B6CE92`
- `kitty123` never gets saved anywhere *in the clear*
- Nearly impossible to go backwards from hash to password

  `hash("89FA210B6CE92") -> A45120BC3EFF74`

Hashes in Login



Mason Username (NetID): jdoe123

Password: ••••••••••••••••••

Legit Login

- Prompt for username/password

  ```
  jdoe123 : kitty123
  ```

- Compute hash of password

  ```
  hash("kitty123")
    -> 89FA210B6C
  ```

- Check for match against saved hash

  ```
  89FA210B6C == 89FA210B6C
  ```

- Allow Login

Failed Login

- Prompt for username/password

  ```
  jdoe123 : doge456
  ```

- Compute hash of password

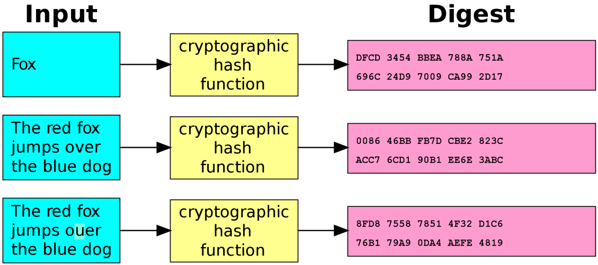
  ```
  hash("doge456")
    -> 8E30FA154
  ```

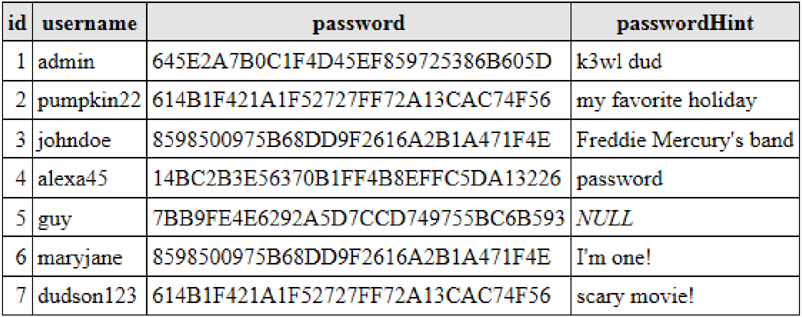
- Check for match against saved hash

  ```
  8E30FA154 != 89FA210B6C
  ```

- Deny Login

Attacking Password Files





id	username	password	passwordHint
1	admin	645E2A7B0C1F4D45EF859725386B605D	k3wl dud
2	pumpkin22	614B1F421A1F52727FF72A13CAC74F56	my favorite holiday
3	johndoe	8598500975B68DD9F2616A2B1A471F4E	Freddie Mercury's band
4	alexa45	14BC2B3E56370B1FF4B8EFFC5DA13226	password
5	guy	7BB9FE4E6292A5D7CCD749755BC6B593	*NULL*
6	maryjane	8598500975B68DD9F2616A2B1A471F4E	I'm one!
7	dudson123	614B1F421A1F52727FF72A13CAC74F56	scary movie!

Picking a Good Password

- Simplest way you can trivially increase security
- Trouble: Required to make frequent changes
  - Makes remembering harder
  - GMU: change every 180 days
  - Compliance with some Virginia State Mandate but can't seem to find where it is written
- Never reveal your password to anyone
- GMU: Passwords are kept encrypted in a secure location and cannot be looked up by anyone (not even the ITU Support Center). (more info)

Password Selection Methods

General Guidelines

Never include personal info that can be looked up

- Your name, family names, birthdays, favorites, car you drive
- Anything on FB is a bad idea
- Any single dictionary word. . .

Two Methods

You have to remember the password; here are two methods

- OK: Sentence Method
  - Traditional method of picking hard passwords
  - Inferior to. . .
- Awesome: CorrectHorseBatteryStaple Method
  - Picking a password that's easy to remember and hard to crack

In-class Credit

Try both of these; which one do you prefer?