9/13/24 CIS 3362

ADFGVX review

① Phase 1 is look up each character in 6x6 grid (key #1) and replace it with a 2 letter pair (row, col) of where the letter is in the grid. (Basically a substitution for 36 character: A-Z, 0-9.

Step 1: AX XF GG FD FA XF DD XD GF DF DD

② Transposition with keyword.

key #2: P A P E R

22/5 → min in col

22 ÷ 5 → # cols extra

P	A	P	E	R
3	1	4	2	5
A	X	X	F	G
G	F	D	F	A
X	F	D	D	X
D	G	F	D	F
D	D			

If you know 22 chars, you know each col size

] sort letters alpha order ties - number left to right

Copy msg into grid row by row, left to right

Read the column in numerical order by ranks

End Step 2: XFFGDFFDDAGXDD XDDFGAXF

When decrypting, remake grid, copy appropriate # letters by col!

Enigma

Used by Germans during WWII.

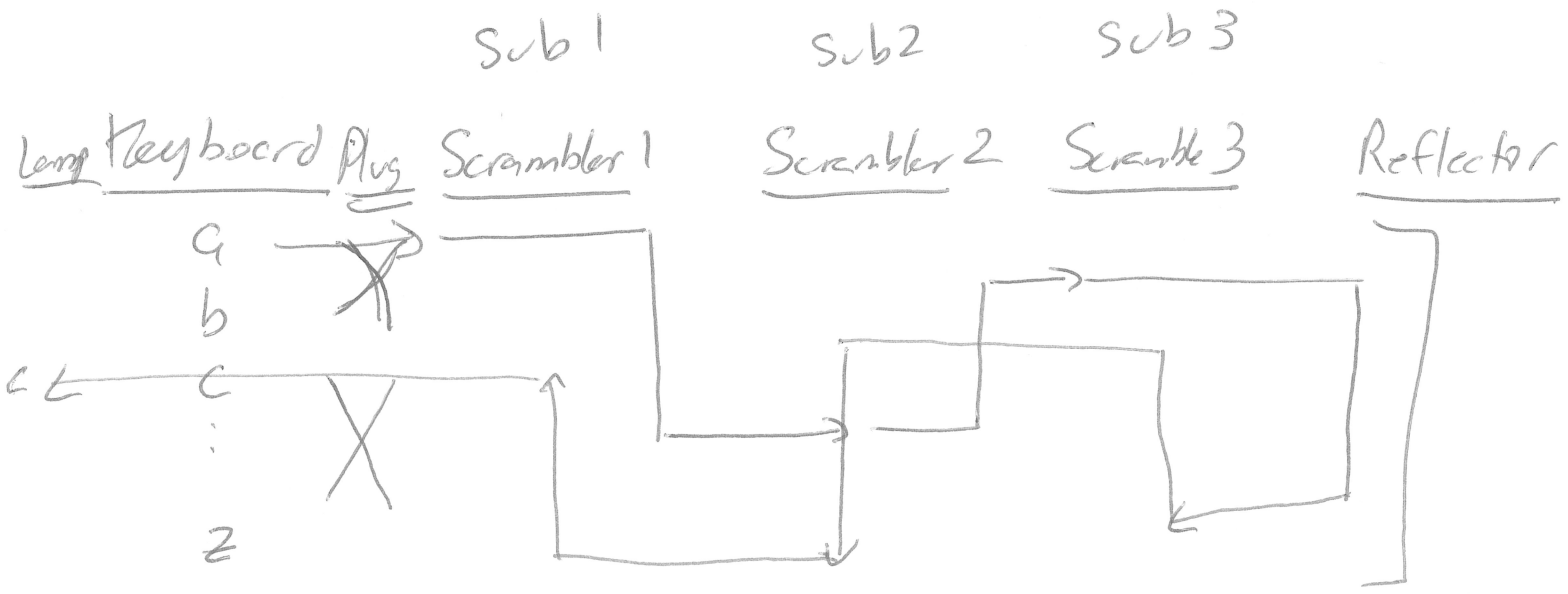
— Imitation Game (movie)

Enigma invented ~1917 - Arthur Scherbius (private business)

Huge step up from Playfair or Hill

(1) How machine is built/works

(2) How Enigma is broken.



Scramblers work like odometer in a car
circular disks + rotate (26 times for a full revolution)

AAA → encrypt one letter

AAB
⋮
AAZ
ABA
⋮
AZZ
BAA
↓
ZZZ

26^3 settings scramblers

Machine uses 26^3 substitution ciphers.
It encrypts one letter w/ one of them, then moves onto the next letter w/ the next key

Imagine Vigenere with a keyword of length $26^3 = 17,576$, but we do a substitution at each letter!

Use of Machine

① Day Code (publish in secret book)
② Msg Code

Jan1 - DQR
Jan2 - XXM
Jan3 - CQB
etc.

1st 6 chars will be the ~~Day~~ Msg code

~~DQRDQR~~

① Set machine to the Day Code (position of scramblers)

L	M	R
S1	S2	S3

② encrypt the message code twice (operator chooses it randomly)

MJP (msg code)

MJPMJP (encrypt DQR)

D	D	D	D	D	D
Q	Q	Q	Q	Q	Q
R	S	T	U	V	W

} current settings

(3) Set machine to the message code

M	Q	R
S1	S2	S3

MSG HELLO

H	E	L	L	O
m	m	m	m	m
Q	Q	Q	Q	Q
R	S	T	U	V

Germans started using for their military in the 20s or early 30s.

Frenchf Polish - Peace Time Pact to share intelligence Info.

~1932 or 1933 French shared info w/ Polish

French secret agent (unknown)

German guy · Hans Thilo Schmidt

- had access to blueprints of Enigma

French agent bribed Hans with lots of money ~ 10,000 francs today. Hans met agent + brought book w/ blue print hotel - french agent took pictures!