

CIS 3362 9/8/2023

let $\rightarrow$ let
combo letters doesn't matter } all old sys including
Vigenere do letter by
letter processing

Next Step "CA" $\rightarrow$ "MD"
etc.
676 possible pairs

26 sub chart $\Rightarrow$ OK by hand
 $676 \times 676 \Rightarrow$ tough

S	A	B	...	Z
A	CP	DA		
B				
C				
...				
Z				

etc.

$\rightarrow$ more complicated but can we create a
system that encrypts 2 letters at a
time and is EASY to use?

$\Rightarrow$ PLAYFAIR

Playfair

① key word ("KNIGHTS")

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

5x5 square

→ if last letter
by itself
add padding
letter...

MSG: "IT IS RAINING NOW LLAMA"

Row shift right 1 spot wrap around rightmost

IT → KA
IS → NA
RA → QB
IN → GJ (can choose)
GN → HI (choose 2. ff)
OW → PV
LX → FY
LA → FB

MA → FC

Box

Box case

c	a
b	d

ab → cd
ba → dc

Column

SP → EW
NW → SN
wrap around
bottom spot

Undo box ⇒ SAME

When decrypting context to choose I or J.

undo row ⇒ go left 1 spot (instead right)

undo col ⇒ go up 1 spot (not down)

Keyword MISSISSIPPI

MISP

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

Decrypting

Identifying a ciphertext as Polyfair:

- ① even length msg
- ② Rare consonants: J, K, Q, X, Z appear quite a bit ciphertext.
- ③ We divided digrams no repeated letters appear.
- ④ freq distribution digraph^{ms} approaches that of english.

Characteristics

- ① a letter ~~is~~ never encrypts as itself
- ② 2 reversed ~~are~~ digrams will be represented as the same pair of letters in reverse.

D	X	DE → X [✓]
Y	E	ED → YX

- ③ every plaintext letter can only be encrypted as one of 5 letters

1	m	2	3	4
	5			

(or wraparound)

How to break

If you have matching plaintext $\leftrightarrow$ ciphertext,

PLAYFAIR $\leftrightarrow$ QKFVGBLE

PL $\rightarrow$ QK

K	L
P	Q



K	L
P	Q

most likely
if guess
right
m, n, o
not in
keyword

~~AF~~ $\rightarrow$ FV
AY

keyword

A	F
KL	
PQ	
V	Y

FA $\rightarrow$ GB (in order for this to work,
same row $\Rightarrow$)

A	B	FG
H	I	J K <u>L</u>
		P Q
V		Y Z

keyword
has 2 letters
from C, D, E

IR $\rightarrow$ LE } R could be next Q OR
in keyword

I $\Rightarrow$ left of K or keyword

L $\Rightarrow$ known

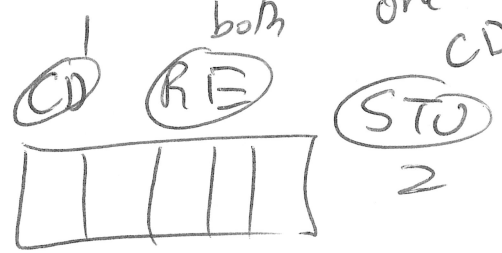
RE same row but _{no} fit $\Rightarrow$ Both in keyword!

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

(RE)

key word
RE, ~~no~~
two letters
of STU
one of
CD

← RSTU



Intended ← "SECRET"
⇒ "SECR T"