

9/13/19 ①

Affine, Shift

Substitution, Vigenere - Monoalphabetic

→ breakable in 19th century

Codestars ⇒ Polyalphabetic

Playfair Cipher

- need to implement by hand

- encrypt more than 1 letter at a time

keyword: "PROBLEMS" // ~~BOOKKEEPER~~
BOKEPR

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

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

1. Split into digraphs

2. Look for doubles
(aa, bb, etc.)

→ insert a padding
char. (Q) - as
needed
left to
right.

SHE WENT TO THE STORE

SH EW EN ~~IT~~ OT HE ST OR E
TQ TO TH ES TO RE

1. If 2 letters are on the same row,
each encrypts to its neighbor to
the right, using wrap-around.

2. If 2 letters are on the same col,
each encrypts to its neighbor below,
using wrap-around.

3. Box Rule



SH → AG
 EW → MV
 EN → MK
 TQ → UT
 TO → QB
 TH → YT
 ES → MA
 TO → QB
 RE → PM

Decryption

JANGLE 9/13/19 (2)

1. Box rule -
opp corners
(same encryption)

J	A	N	G	L	E

2. Row -
go left
instead of
right

3. Col -
go up instead of down

How to break Playfair?

① ~~Also~~ Much easier if you have a
little matching plain/cipher text.

Plain: A S A M P L E
 Cipher: P K K M K M E

Can't be
Playfair

Plain: A S A M P L E
 Cipher: E W D W Q N B

↙ ↘
 Some row Some row
 col col
 box? box