RECAP: ~ ADFGX & ADFGVX ciphers.

~ Permutation cipher.

- Use of password

Playfair cipher

Use pass word to prepare the table

PASSWORD is the password

alphabetically put them : ADOPRSW

Standard

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

password

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

Encryption: $\Sigma : P \to C$

- Pair consecutive characters starting from the 1st character.

MOVE FORWARD ::

(1) If X_1, X_2 are diagonally opposite on the above table then find Y_1, Y_2, diagonally opposite for the same rectangle

Y_1 & X_1 are on the same column

& Y_2 & X_2 " " " column.

(2) If X_1, X_2 are on the same row, apply right cyclic 1-shift & get $Y_1 Y_2$

- If $X_1 X_2$ are on the same column then downward cyclic 1-shift is to be applied & get $Y_1 Y_2$

- If $X_1 = X_2$, then insert X between X_1 & X_2 & do pairing as $X_1 X$ & X_2 ..... & then apply the other rules for encryption.

MO → DN

VE → WZ

FO → AH

RW → ED

AR → DA

D : → VO

- Decryption rules $Y_1 Y_2$ - - - -.

(1') = (1)

(2') apply left cyclic 1-shift if Y_1 & Y_2 are on the same row on the table.

(3') apply upward cyclic 1-shift if Y_1 & Y_2 are on the same column on the table.

Table

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

Decrypt (playfair ciphers)

RD ZP TP DM QA ZP

HCF = GCD

Coprime or relatively prime a, b $\gcd(a,b) = 1$

also denoted by (a,b)

Defining properties

- $d = \gcd(a,b)$
- $d|a, d|b$
- if $c|a, c|b$, then $c|d$.

Lemma: if $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$.

(write - proof)

Thm: if $a, b \in \mathbb{Z}$, at least one of them is non zero then $\gcd(a,b)$ exists & $\gcd(a,b) = xa + yb$ for some $x, y \in \mathbb{Z}$. Infact $\gcd(a,b)$ is the least positive integer which can be written in the form $sa + tb$ for $s, t \in \mathbb{Z}$.

→ WLG, $b \geq 0$.

Proof: Consider $S = \{sa+tb : sa+tb > 0,\ s,t \in \mathbb{Z}\} \subset \mathbb{N}$

Well ordering principle S has a least member

$S \neq \phi$ because take $t=1$ $s=0$

$b \in S$.

If $\gcd(a,-b)$ exists then $\gcd(a,b)$ exists & $\gcd(a,b) = \gcd(a,-b)$

Let $d = xa+yb$ be the least member of S.

Now show that $d = \gcd(a,b)$.

Step 1: $d|a$ Step 2: $d|b$ Step 3: $c|a, c|b \Rightarrow c|d$.

If $d \nmid a$, then $a = dq + r \Rightarrow r = a - dq > 0$

$r = a - (xa+yb)q$

$= (1-xq)a + (-yq)b$.

since $r < d$

$r \in S$ a contradiction

Euclidean algorithm

$\alpha, \beta \in \mathbb{Z}$, $\beta > 0$

$\alpha = \beta q + r$

where $q, r \in \mathbb{Z}$

& $0 \leq r < \beta$.

So $r = 0$

so that $d|a$.

Similarly $d|b$.

So d is the $\gcd(a,b)$

Algorithm. Assume $b > 0$. Apply Euclidean algorithm if $r_1 = 0$ $\gcd(a,b) = b$ else.

$a = bq_1 + r_1$

$b = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$\vdots$

$r_{k-2} = r_{k-1} q_k + r_k$

$\vdots$

$r_{k-1} = r_k q_{k+1} + r_{k+1}$

$r_k = r_{k+1} q_{k+2} + r_{k+2}$ & $r_{k+2} = 0$,

For some k, $r_{k+2} = 0$ $\rightsquigarrow$ $b = r_1 > r_2 > \cdots \geq 0$.

Then $\gcd(a,b) = r_{k+1}$

$\gcd(a,b) = \gcd(b,r)$

$a = bq + r$.

$$r_{k+1} = \gcd(r_k, r_{k+1})$$
$$= \gcd(r_{k-1}, r_k)$$
$$= \gcd(r_{k-2}, r_{k-1})$$
$$\vdots$$
$$= \gcd(a,b)$$

Find $\gcd(3026, 445) =$

$3026 = 445 \times 6 + 356$.

$445 = 356 \times 1 + 89$

$356 = 89 \times 4 + 0$

$\gcd(3026, 445) = 89$

Suppose $n > 1$ fixed. $m \in \mathbb{N}$.

Write $m = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 =: p_k(n)$

where $a_k \neq 0$, $0 \leq a_0, a_1, \ldots, a_k \leq n-1$

for some k.

$p_k(n) \in \mathbb{Z}$.

$\deg(p_k(n)) = k$.

$n^k \leq m \leq n^{k+1} - 1 \leq n^{k+1}$

$$\log_n(n^k) \leq \log_n m \Rightarrow k \leq \log_n m \leq k+1$$

$$\boxed{k = \lfloor \log_n m \rfloor + 1.}$$