Practice01

Friday, March 3, 2023 1:47 PM

$$\begin{tikzcd}
\Sigma \arrow[d, leftrightarrow] & = \{ a, \arrow[d, leftrightarrow] & b, \arrow[d, leftrightarrow] & c, \ldots, z, & \sqcup \} \arrow[d, leftrightarrow] \\
I & = \{ 0, & 1, & 2, \ldots\ldots 25, & 26 \}
\end{tikzcd}$$

27 letters

— o —

SHIFT CIPHER

0 1 2 3 4 5 6
a b c d e f
c d e f a b
2 3 4 5 0 1

$k = C = 2$

m = deadbeef
cipher = facfdaab

$m \in \Sigma^n$
$k \in \Sigma$

ENCRYPT: $C[i] = (m[i] + k) \mod \ell$
DECRYPT: $m[i] = (c[i] - k) \mod \ell$

key

lenght of alphabet (27)

— o —

Vigenère-cipher

abcdef

key = bcd (bcd bcd bcd...)...

abcdef
bcdefa
efabcd
defabc

key = bed (bedbedbed...)...
143

m = deadbeef

c = ecdefafd

012345
123450
450123
345012

k = 143

m = 311325

c = 454402

$m \in \Sigma^n$, $k \in \Sigma^p$

ENCRYPT $c[i] = (m[i] + k[i \bmod p]) \bmod \ell$

DECRYPT $m[i] = (c[i] - k[i \bmod p]) \bmod \ell$