Affine Cipher

Enkripsi   Aku suka makan keju $a = 9$ $b = 10$

A	k	u	S	u	k	A	M	A	k	A	N	K	E	J	U
0	10	20	18	20	10	0	12	0	10	0	13	10	4	9	20

$E(x) = (ax + b) \bmod 26)$

$E(0) = (9 \cdot 0 + 10) \bmod 26 = 10 \Rightarrow k$

$E(10) = (9 \cdot 10 + 10) \bmod 26 = 22 \Rightarrow w$

$E(20) = (9 \cdot 20 + 10) \bmod 26 = 8 \Rightarrow i$

$E(18) = (9 \cdot 18 + 10) \bmod 26 = 16 \Rightarrow Q$

$E(20) = (9 \cdot 20 + 10) \bmod 26 = 8 \Rightarrow i$

$k(10) = (9 \cdot 10 + 10) \bmod 26 = 22 \Rightarrow w$

$k(0) = (9 \cdot 0 + 10) \bmod 26 = 10 \Rightarrow k$

$k(12) = (9 \cdot 12 + 10) \bmod 26 = 14 \Rightarrow o$

$k(0) = (9 \cdot 0 + 10) \bmod 26 = 10 \Rightarrow k$

$k(10) = (9 \cdot 10 + 10) \bmod 26 = 22 \Rightarrow w$

$k(0) = (9 \cdot 0 + 10) \bmod 26 = 10 \Rightarrow k$

$k(13) = (9 \cdot 13 + 10) \bmod 26 = 23 \Rightarrow x$

$k(10) = (9 \cdot 10 + 10) \bmod 26 = 22 \Rightarrow w$

$k(4) = (9 \cdot 4 + 10) \bmod 26 = 20 \Rightarrow u$

$k(9) = (9 \cdot 9 + 10) \bmod 26 = 13 \Rightarrow N$

$k(20) = (9 \cdot 20 + 10) \bmod 26 = 8 \Rightarrow i$

Aku suka makan keju $\Rightarrow$ kwi Qiwk okwkx wuNi

Dekripsi

mencari a^{-1}

$GCD(a, m)$

$gcd(9, 26)$

$26 = 9 \times 2 + 8$ $\quad t_0 = 0, \; t_1 = 1$

$9 = 8 \times 1 + 1$ $\quad t_2 = (t_0 - (q_1 . t_1)) \bmod 26$

$8 = 1 \times 8 + 0$ $\quad = (0 - (2 . 1)) \bmod 26 = -2 \bmod 26 = 24$

$t_3 = (t_1 - (q_2 . t_2)) \bmod 26$

$= (1 - (1 . 24)) \bmod 26 = -23 \bmod 26 = 3$

$a^{-1} = 3$

$D(y) = a^{-1}(y - b) \bmod 26$

$D(10) = 3(10 - 10) \bmod 26 = 0 \Rightarrow A$

$D(22) = 3(22 - 10) \bmod 26 = 10 \Rightarrow K$

$D(8) = 3(8 - 10) \bmod 26 = 20 \Rightarrow U$

$D(16) = 3(16 - 10) \bmod 26 = 18 \Rightarrow S$

$D(8) = 3(3 - 10) \bmod 26 = 20 \Rightarrow U$

$D(22) = 3(22 - 10) \bmod 26 = 10 \Rightarrow K$

$D(10) = 3(10 - 10) \bmod 26 = 0 \Rightarrow A$

$D(14) = 3(14 - 10) \bmod 26 = 12 \Rightarrow M$

$D(10) = 3(10 - 10) \bmod 26 = 0 \Rightarrow A$

$D(22) = 3(22 - 10) \bmod 26 = 10 \Rightarrow K$

$D(10) = 3(10 - 10) \bmod 26 = 0 \Rightarrow A$

$D(23) = 3(23 - 10) \bmod 26 = 13 \Rightarrow N$

Scanned with CamScanner

No.

Date :

$D(22) = 3(22-10) \bmod 26 = 10 \Rightarrow K$

$D(20) = 3(20-10) \bmod 26 = 4 \Rightarrow E$

$D(13) = 3(13-10) \bmod 26 = 9 \Rightarrow J$

$D(8) = 3(8-10) \bmod 26 = 20 \Rightarrow U$

Aku suka makan keju

Scanned with CamScanner