```
[ TUGAS AFFINE CIPHER ]

P  R  A  M  E  S    R  A  Y    L  A  P  I  A  N
15 17 0  12 4  18   17 0  24   11 0 15  8  0  13

a = 9
b = 59

E(x) = (ax + b) mod 26
[P] = (9.15 + 59)       mod 26 = 194    mod 26 = 12     -> [M]
[R] = (9.17 + 59)       mod 26 = 212    mod 26 = 4      -> [E]
[A] = (9.0 + 59)        mod 26 = 59     mod 26 = 7      -> [H]
[M] = (9.12 + 59)       mod 26 = 167    mod 26 = 11     -> [L]
[E] = (9.4 + 59)        mod 26 = 59     mod 26 = 7      -> [H]
[S] = (9.18 + 59)       mod 26 = 221    mod 26 = 13     -> [N]

[R] = (9.17 + 59)       mod 26 = 212    mod 26 = 4      -> [E]
[A] = (9.0 + 59)        mod 26 = 59     mod 26 = 7      -> [H]
[Y] = (9.24 + 59)       mod 26 = 275    mod 26 = 15     -> [P]

[L] = (9.11 + 59)       mod 26 = 158    mod 26 = 2      -> [C]
[A] = (9.0 + 59)        mod 26 = 59     mod 26 = 7      -> [H]
[P] = (9.15 + 59)       mod 26 = 194    mod 26 = 12     -> [M]
[I] = (9.8 + 59)        mod 26 = 131    mod 26 = 1      -> [B]
[A] = (9.0 + 59)        mod 26 = 59     mod 26 = 7      -> [H]
[N] = (9.13 + 59)       mod 26 = 176    mod 26 = 20     -> [U]

E(x) = M E H L H N   E H P   C H M B H U


D(y) = a^-1 (y - b) mod 26

Mencari a^-1:
GCD(a, m) = GCD(9, 26)
26      = 9 * 2 + 8
9       = 8 * 1 + 1
8       = 1 * 8 + 0

t0      = 0
t1      = 1
t2      = (t0 - (q1 . t1))      mod 26
        = (0 - (2 * 1))         mod 26
        = (0 - 2)               mod 26
        = -2                    mod 26
        = 24
t3      = (t1 - (q2 . t2))      mod 26
        = (1 - (1 * 24))        mod 26
        = (1 - 24)              mod 26
        = -23                   mod 26
        = 3
```

```
a^-1    = 3

[M] = a^-1 (12 - 59)    mod 26 = 3 * -47        mod 26 = 15     -> [P]
[E] = a^-1 (4 - 59)     mod 26 = 3 * -55        mod 26 = 17     -> [R]
[H] = a^-1 (7 - 59)     mod 26 = 3 * -52        mod 26 = 0      -> [A]
[L] = a^-1 (11 - 59)    mod 26 = 3 * -48        mod 26 = 12     -> [M]
[H] = a^-1 (7 - 59)     mod 26 = 3 * -52        mod 26 = 4      -> [E]
[N] = a^-1 (13 - 59)    mod 26 = 3 * -46        mod 26 = 18     -> [S]

[E] = a^-1 (4 - 59)     mod 26 = 3 * -55        mod 26 = 17     -> [R]
[H] = a^-1 (7 - 59)     mod 26 = 3 * -52        mod 26 = 0      -> [A]
[P] = a^-1 (15 - 59)    mod 26 = 3 * -44        mod 26 = 24     -> [Y]

[C] = a^-1 (2 - 59)     mod 26 = 3 * -57        mod 26 = 11     -> [L]
[H] = a^-1 (7 - 59)     mod 26 = 3 * -52        mod 26 = 0      -> [A]
[M] = a^-1 (12 - 59)    mod 26 = 3 * -47        mod 26 = 15     -> [P]
[B] = a^-1 (1 - 59)     mod 26 = 3 * -58        mod 26 = 8      -> [I]
[H] = a^-1 (7 - 59)     mod 26 = 3 * -52        mod 26 = 0      -> [A]
[U] = a^-1 (20 - 59)    mod 26 = 3 * -39        mod 26 = 13     -> [N]

D(x) = P R A M E S   R A Y   L A P I A N
```