Tugas Praktikum Kriptografi #2

Nama : Andyka Baswara Putra

NPM : 140810200061

Kelas : A

Kalimat Sederhana

ANDYKA BASWARA PUTRA

0 13 3 24 10 0 1 0 18 22 0 17 0 15 20 19 17 0

Nilai a = 1, b = 10

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

E(13) = (1(13) + 10) mod 26 = 23 mod 26 = 23 > X

E(3) = (1(3) + 10) mod 26 = 13 mod 26 = 13 > N

E(24) = (1(24) + 10) mod 26 = 34 mod 26 = 8 > I

E(10) = (1(10) + 10) mod 26 = 20 mod 26 = 20 > U

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

E(1) = (1(1) + 10) mod 26 = 11 mod 26 = 11 > L

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

E(18) = (1(18) + 10) mod 26 = 28 mod 26 = 10 > C

E(22) = (1(22) + 10) mod 26 = 32 mod 26 = 6 > G

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

E(17) = (1(17) + 10) mod 26 = 27 mod 26 = 1 > B

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

E(15) = (1(15) + 10) mod 26 = 25 mod 26 = 25 > Z

E(20) = (1(20) + 10) mod 26 = 30 mod 26 = 4 > E

E(19) = (1(19) + 10) mod 26 = 29 mod 26 = 3 > D

E(17) = (1(17) + 10) mod 26 = 27 mod 26 = 1 > B

E(0) = (1(0) + 10) mod 26 = 10 mod 26 = 10 > K

ANDYKA BASWARA PUTRA > E(x) = KXNIUK LKCGKBK ZEDBK

Deskripsi

Mencari a-1 :

GCD(a, m)

Gcd(1,26)

26 = 1 * 26 + 0

T0 = 0, T1 = 1

T2 = (t0 – (q1 . t1)) mod 26

= (0-(26.1) mod 26 = -26 mod 26 = 1

a-1 = 1

KXNIUK LKCGKBK ZEDBK

10 23 13 8 20 10 11 10 2 22 10 1 10 25 4 3 1 10

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

D(23) = 1(23-10) mod 26 = 13 mod 26 = 13 > N

D(13) = 1(13-10) mod 26 = 3 mod 26 = 3 > D

D(8) = 1(8-10) mod 26 = -2 mod 26 = 24 > Y

D(20) = 1(20-10) mod 26 = 10 mod 26 = 10 > K

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

D(11) = 1(11-10) mod 26 = 1 mod 26 = 1 > B

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

D(2) = 1(2-10) mod 26 = -8 mod 26 = 0 > S

D(6) = 1(6-10) mod 26 = -4 mod 26 = 22 > W

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

D(1) = 1(1-10) mod 26 = -9 mod 26 = 17 > R

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

D(25) = 1(25-10) mod 26 = 15 mod 26 = 15 > P

D(4) = 1(4-10) mod 26 = -6 mod 26 = 20 > U

D(3) = 1(3-10) mod 26 = -7 mod 26 = 19 > T

D(1) = 1(1-10) mod 26 = -9 mod 26 = 17 > R

D(10) = 1(10-10) mod 26 = 0 mod 26 = 0 > A

KXNIUK LKCWKBK ZEDBK > D(x) = ANDYKA BASWARA PUTRA