**Tugas 2**

Nama : Patricia Joanne

NPM : 140810160065

**26 September 2018**

**Buatlah satu kalimat singkat yang akan dienkripsi dan kemudian dekripsikan kembali, menggunakan Affine Cipher**

**a = 19**

**b = 20**

**Note:**

**Setiap orang beda kalimat, minimal 3 kata (huruf semua, tanpa angka atau tanda baca)**

**Spasi tidak dienkripsi**

Plain Text:

**PAK AKIK MENGAJAR KRIPTOGRAFI**

15-0-10 0-10-8-10 12-4-13-6-0-9-0-17 10-17-8-15-19-14-6-17-0-5-8

Enkripsi: e(x) = (ax+b) mod 26

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Huruf Awal | x | Rumus Enkripsi | e(x) | Huruf Hasil |
| P | 15 | (19\*15+20) mod 26 | 19 | T |
| A | 0 | (19\*0+20) mod 26 | 20 | U |
| K | 10 | (19\*10+20) mod 26 | 2 | C |
| A | 0 | (19\*0+20) mod 26 | 20 | U |
| K | 10 | (19\*10+20) mod 26 | 2 | C |
| I | 8 | (19\*8+20) mod 26 | 16 | Q |
| K | 10 | (19\*10+20) mod 26 | 2 | C |
| M | 12 | (19\*12+20) mod 26 | 14 | O |
| E | 4 | (19\*4+20) mod 26 | 18 | S |
| N | 13 | (19\*13+20) mod 26 | 7 | H |
| G | 6 | (19\*6+20) mod 26 | 4 | E |
| A | 0 | (19\*0+20) mod 26 | 20 | U |
| J | 9 | (19\*9+20) mod 26 | 9 | J |
| A | 0 | (19\*0+20) mod 26 | 20 | U |
| R | 17 | (19\*17+20) mod 26 | 5 | F |
| K | 10 | (19\*10+20) mod 26 | 2 | C |
| R | 17 | (19\*17+20) mod 26 | 5 | F |
| I | 8 | (19\*8+20) mod 26 | 16 | Q |
| P | 15 | (19\*15+20) mod 26 | 19 | T |
| T | 19 | (19\*19+20) mod 26 | 17 | R |
| O | 14 | (19\*14+20) mod 26 | 0 | A |
| G | 6 | (19\*6+20) mod 26 | 4 | E |
| R | 17 | (19\*17+20) mod 26 | 5 | F |
| A | 0 | (19\*0+20) mod 26 | 20 | U |
| F | 5 | (19\*5+20) mod 26 | 11 | L |
| I | 8 | (19\*8+20) mod 26 | 16 | Q |

Cipher Text: **TUCUCQCOSHEUJUFCFQTRAEFULQ**

Dekripsi: d(y) = a-1 (y-b) mod 26

a-1 = gcd (19,26) = 1

19-1 = 11

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Huruf Awal | y | Rumus Dekripsi | d(y) | Huruf Hasil |
| T | 19 | 11\*(19-20) mod 26 | 15 | P |
| U | 20 | 11\*(20-20) mod 26 | 0 | A |
| C | 2 | 11\*(2-20) mod 26 | 10 | K |
| U | 20 | 11\*(20-20) mod 26 | 0 | A |
| C | 2 | 11\*(2-20) mod 26 | 10 | K |
| Q | 16 | 11\*(16-20) mod 26 | 8 | I |
| C | 2 | 11\*(2-20) mod 26 | 10 | K |
| O | 14 | 11\*(14-20) mod 26 | 12 | M |
| S | 18 | 11\*(18-20) mod 26 | 4 | E |
| H | 7 | 11\*(7-20) mod 26 | 13 | N |
| E | 4 | 11\*(4-20) mod 26 | 6 | G |
| U | 20 | 11\*(20-20) mod 26 | 0 | A |
| J | 9 | 11\*(9-20) mod 26 | 9 | J |
| U | 20 | 11\*(20-20) mod 26 | 0 | A |
| F | 5 | 11\*(5-20) mod 26 | 17 | R |
| C | 2 | 11\*(2-20) mod 26 | 10 | K |
| F | 5 | 11\*(5-20) mod 26 | 17 | R |
| Q | 16 | 11\*(16-20) mod 26 | 8 | I |
| T | 19 | 11\*(19-20) mod 26 | 15 | P |
| R | 17 | 11\*(17-20) mod 26 | 19 | T |
| A | 0 | 11\*(0-20) mod 26 | 14 | O |
| E | 4 | 11\*(4-20) mod 26 | 6 | G |
| F | 5 | 11\*(5-20) mod 26 | 17 | R |
| U | 20 | 11\*(20-20) mod 26 | 0 | A |
| L | 11 | 11\*(11-20) mod 26 | 5 | F |
| Q | 16 | 11\*(16-20) mod 26 | 8 | I |

Plain Text: **PAKAKIKMENGAJARKRIPTOGRAFI**