Nama : Aidil Fitra

NPM : 140810190053

Tugas 2 Praktikum Kriptografi

1. Exercise

* Enkripsi Shift Cipher ‘FORTRAN’, k=20

Plain text

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| F | O | R | T | R | A | N |
| 5 | 14 | 17 | 19 | 17 | 0 | 13 |

Hasil enkripsi

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 25 | 8 | 11 | 13 | 11 | 20 | 7 |
| Z | I | L | N | L | U | H |

* Dekripsi shift cipher ‘ZGXEIDZJN’, k=15

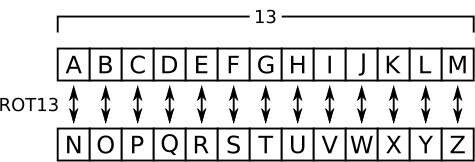
Cipher text

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Z | G | X | E | I | D | Z | J | N |
| 25 | 6 | 23 | 4 | 8 | 3 | 25 | 9 | 13 |

Hasil dekripsi

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 17 | 8 | 15 | 19 | 14 | 10 | 20 | 24 |
| K | R | I | P | T | O | K | U | Y |

* Dekripsi ‘TNZCNATXNA’ dengan ROT13



TNZCNATXNA → GAMPANGKAN

1. Kalimat sederhana (min 3 kata & total min 15 huruf), enkripsikan dengan Affine Cipher dan kembalikan menjadi plainteks

Plainteks: AIDIL BUTUH MINUM

Kunci: (a = 5, b = 2)

* + Ekripsi

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | I | D | I | L | B | U | T | U | H | M | I | N | U | M |
| 0 | 8 | 3 | 8 | 11 | 1 | 20 | 19 | 20 | 7 | 12 | 8 | 13 | 20 | 12 |

Enkripsikan menggunakan rumus

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 8 | 3 | 8 | 11 | 1 | 20 | 19 | 20 | 7 | 12 | 8 | 13 | 20 | 12 |
| 2 | 16 | 17 | 16 | 5 | 7 | 24 | 19 | 24 | 11 | 10 | 16 | 15 | 24 | 10 |

Ubah menjadi cipherteks

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 16 | 17 | 16 | 5 | 7 | 24 | 19 | 24 | 11 | 10 | 16 | 15 | 24 | 10 |
| C | Q | R | Q | F | H | Y | T | Y | L | K | Q | P | Y | K |

Maka didapatkan cipherteksnya: CQRQFHYTYLKQPYK

* + Dekripsi

Ubah cipherteks

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | Q | R | Q | F | H | Y | T | Y | L | K | Q | P | Y | K |
| 2 | 16 | 17 | 16 | 5 | 7 | 24 | 19 | 24 | 11 | 10 | 16 | 15 | 24 | 10 |

Dekripsi menggunakan rumus

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 16 | 17 | 16 | 5 | 7 | 24 | 19 | 24 | 11 | 10 | 16 | 15 | 24 | 10 |
| 0 | 8 | 3 | 8 | 11 | 1 | 20 | 19 | 20 | 7 | 12 | 8 | 13 | 20 | 12 |

Ubah menjadi plainteks

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 8 | 3 | 8 | 11 | 1 | 20 | 19 | 20 | 7 | 12 | 8 | 13 | 20 | 12 |
| A | I | D | I | L | B | U | T | U | H | M | I | N | U | M |

Maka hasil dari dekripsinya: AIDILBUTUHMINUM