Nama : Ilmi Faizan

NIM : E1E120011

Mata Kuliah : Kriptografi

Enkripsi kalimat “teknik informatika uho” menggunakan metode Caesar cipher (subtitusi (gunakan rumus persamaan dengan pergeseran n = 5 (Enkripsi: *c* = *E*(*p*) = (*p* + n) mod 26)) dan transposisi (gunakan rumus yang ada di ppt kriptografi klasik hal 31)), vigenere cipher (gunakan rumus yang ada di ppt kriptografi klasik 2) dan playfair cipher (gunakan rumus yang ada di ppt kriptografi klasik 2)

* Caesar Cipher

|  |  |
| --- | --- |
| A = 0 | n = 5 |
| B = 1 | Plaintext = teknik informatika uho |
| C = 2 | Persamaan = *c* = *E*(*p*) = (*p* + 5) mod 26 |
| … |  |
| Z = 25 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| t | = 19 | *c1 = E(19) = (19 + 5) mod 26* | = 24 | = y |
| e | = 4 | *c2 = E(4) = (4 + 5) mod 26* | = 9 | = j |
| k | = 10 | *c3 = E(10) = (10 + 5) mod 26* | = 15 | = p |
| n | = 13 | *c4 = E(13) = (13 + 5) mod 26* | = 18 | = s |
| i | = 8 | *c5 = E(8) = (8 + 5) mod 26* | = 14 | = n |
| k | = 10 | *c6 = E(10) = (10 + 5) mod 26* | = 15 | = p |
|  |  |  |  |  |
| i | = 8 | *c7 = E(8) = (8 + 5) mod 26* | = 13 | = n |
| n | = 13 | *c8 = E(13) = (13 + 5) mod 26* | = 18 | = s |
| f | = 5 | *c9 = E(5) = (5 + 5) mod 26* | = 10 | = k |
| o | = 14 | *c10 = E(14) = (14 + 5) mod 26* | = 19 | = t |
| r | = 17 | *c11 = E(17) = (17 + 5) mod 26* | = 22 | = w |
| m | = 12 | *c12 = E(12) = (12 + 5) mod 26* | = 17 | = r |
| a | = 0 | *c13 = E(0) = (0 + 5) mod 26* | = 5 | = f |
| t | = 19 | *c14 = E(19) = (19 + 5) mod 26* | = 24 | = y |
| i | = 8 | *c15 = E(8) = (8 + 5) mod 26* | = 13 | = n |
| k | = 10 | *c16 = E(10) = (10 + 5) mod 26* | = 15 | = p |
| a | = 0 | *c17 = E(0) = (0 + 5) mod 26* | = 5 | = f |
|  |  |  |  |  |
| u | = 20 | *c18 = E(20) = (20 + 5) mod 26* | = 25 | = z |
| h | = 7 | *c19 = E(7) = (7 + 5) mod 26* | = 12 | = m |
| o | = 14 | *c20 = E(14) = (14 + 5) mod 26* | = 19 | = t |
|  |  |  |  |  |
| Ciphertext = **YJPSNP NSKTWRFYNPF ZMT** | | | | |

* Cipher Transposisi

Plaintext = teknik informatika uho

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| t | e | k | n | i | k | i | n | f | o | r | m | a | t | i | k | a | u | h | o | a | b | c | d |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | e | k | i | n | k | i | t | k | o | r | a | m | t | i | f | d | u | h | a | o | b | c | a |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Ciphertext = **nekinkitkoramtifduhaobca**

* Vigere Chipher

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | = | t | e | k | n | i | k |  | i | n | f | o | r | m | a | t | i | k | a |  | u | h | o |
| Kunci | = | s | o | n | y | s | o |  | n | y | s | o | n | y | s | o | n | y | s |  | o | n | y |

|  |  |  |  |
| --- | --- | --- | --- |
| (t + s) mod 26 | = (19 + 18) mod 26 | = 37 mod 26 = 11 | = l |
| (e + s) mod 26 | = (4 + 14) mod 26 | = 18 mod 26 = 18 | = s |
| (k + s) mod 26 | = (10 + 13) mod 26 | = 23 mod 26 = 23 | = x |
| (n + s) mod 26 | = (13 + 24) mod 26 | = 37 mod 26 = 11 | = l |
| (i + s) mod 26 | = (8 + 18) mod 26 | = 26 mod 26 = 0 | = a |
| (k + s) mod 26 | = (10 + 14) mod 26 | = 24 mod 26 = 24 | = y |
|  |  |  |  |
| (i + s) mod 26 | = (8 + 13) mod 26 | = 21 mod 26 = 21 | = v |
| (n + s) mod 26 | = (13 + 24) mod 26 | = 37 mod 26 = 11 | = l |
| (f + s) mod 26 | = (5 + 18) mod 26 | = 23 mod 26 = 23 | = x |
| (o + s) mod 26 | = (14 + 14) mod 26 | = 28 mod 26 = 2 | = c |
| (r + s) mod 26 | = (17 + 13) mod 26 | = 30 mod 26 = 4 | = e |
| (m + s) mod 26 | = (12 + 24) mod 26 | = 36 mod 26 = 10 | = k |
| (a + s) mod 26 | = (0 + 18) mod 26 | = 18 mod 26 = 18 | = s |
| (t + s) mod 26 | = (19 + 14) mod 26 | = 33 mod 26 = 7 | = h |
| (i + s) mod 26 | = (8 + 13) mod 26 | = 21 mod 26 = 21 | = v |
| (k + s) mod 26 | = (10 + 24) mod 26 | = 34 mod 26 = 8 | = i |
| (a + s) mod 26 | = (0 + 18) mod 26 | = 18 mod 26 = 18 | = s |
|  |  |  |  |
| (u + s) mod 26 | = (20 + 14) mod 26 | = 34 mod 26 = 8 | = i |
| (h + s) mod 26 | = (7 + 13) mod 26 | = 20 mod 26 = 20 | = u |
| (o + s) mod 26 | = (14 + 24) mod 26 | = 38 mod 26 = 12 | = m |
|  |  |  |  |

Chipertext = **lsxlay vlxcekshvis ium**

* Playfair Chipher

Plaintext = teknik informatika uho

Bigram = te kn ik in fo rm at ik au ho

Kunci =

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | L | N | G | E |
| S | H | P | U | B |
| C | D | F | I | K |
| M | O | Q | R | T |
| V | W | X | Y | Z |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| te => zb   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | rm => to   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | Chipertext :  **zb ef kc fg dq to em kc gs dw** |
| kn => fe   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | at => em   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | |  |
| ik => kc   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | ik => kc   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | |  |
| in => fg   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | au => gs   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | |  |
| fo => dq   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | | ho => dw   |  |  |  |  |  | | --- | --- | --- | --- | --- | | A | L | N | G | E | | S | H | P | U | B | | C | D | F | I | K | | M | O | Q | R | T | | V | W | X | Y | Z | |  |