MATA KULIAH : KEAMANAN KOMPUTER

TUGAS : MEMBUAT APLIKASI ENKRIPSI DAN DEPKRIPSI

ANGGOTA KELOMPOK :

(XXXXXXXX) MUHAMMAD RIDWAN HASIBUAN

(27113817) RISKY PARMANA PUTRA

(28113205) SALIM HAMUD BALFAS

(29113444) YODI SATRIANI

**Enkripsi dan Dekripsi**

Enkripsi, *encrypt* atau *encryption* berasal dari bahasa yunani yaitu kryptos yang artinya tersembunyi atau rahasia. Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasi terjaga dan tidak dapat dibaca tanpa di dekripsi (*decrypt*) dahulu. Enkripsi merupakan proses pengamanan suatu data yang disembunyikan atau konversi data (*plaintext*) menjadi bentuk yang tidak dapat dibaca atau dimengerti. Bentuk konversi data yang telah dienkripsi disebut *ciphertext*. Pesan c*iphertext* merupakan informasi dari seluruh pesan *plaintext*, tetapi tidak dalam format yang dapat dibaca manusia atau komputer tanpa mekanisme yang tepat untuk melakukan dekripsi. Dekripsi adalah proses kebalikan dari enkripsi yaitu mengubah pesan *ciphertext* menjadi *plaintext* kembali menjadi data asli sehingga dapat dibaca atau dimengerti kembali.

Plaintext ciphertext Plaintext

dekripsi

Enkripsi

metode (kunci) metode (kunci)

Proses enkripsi dan dekripsi yaitu, data atau informasi yang akan dienkripsi (*plaintext*) diacak oleh suatu metode (kunci) yang telah ditentukan, kemudian output dari enkripsi (*ciphertext*) dikembalikan ke bentuk asli oleh sebuah metode (kunci) yang sama.

**Metode Enkripsi dan Dekripsi**

Pada aplikasi enkripsi dan dekripsi ini menggunakan beberapa metode, yaitu:

* Substitution Encrypt dan Substitution Decrypt
* Block Encrypt dan Block Decrypt
* Permutation Encrypt dan Permutation Decrypt
* Expansion Encrypt dan Expansion Decrypt
* Compaction Encrypt dan Compaction Decrypt

Substitution Encrypt dan Substitution Decrypt

Metode substitution merupakan metode penggantian setiap karakter *plaintext* dengan karakter lain berdasarkan suatu cara atau rumus tertentu.

Contoh :

Plaintext (encrypt) : aplikasi salcrypt

kunci : [“a”, “g”], [“c”, “u”], [“i”, “x”], [“k”, “d”], [“l”, “5”], [“p”, “i”], [“r”, “1”], [“s”, “6”], [“t”, “h”],

[“y”, “m”], [“ ”, “ ”]

Ciphertext : gi5xdg6x 6g5u1mih **(gambar)**

Plaintext (decrypt) : aplikasi salcrypt **(gambar)**

Block Encrypt dan Block Decrypt

Metode block encrypt ini adalah membagi karakter plaintext ke dalam blok-blok kemudian karakter di enkripsikan secara terpisah terhadap masing-masing blok data. Pada block encrypt ini, blok mempunyai 4 kolom karakter diurutkan dari blok kiri ke kanan, kemudian dienkripsikan dari blok atas kiri ke blok bawah kanan.

Contoh :

Plaintext : salim hamud balfas

plaintext

|  |  |  |  |
| --- | --- | --- | --- |
| s | a | l | i |
| m |  | h | a |
| m | u | d |  |
| b | a | l | f |
| a | s |  |  |

Pembagian blok: plaintext diurutkan dari kiri ke kanan

Ciphertext : smmbaa\*uaslhdlia\*f

|  |  |  |  |
| --- | --- | --- | --- |
| s | a | l | I |
| m | \* | h | A |
| m | u | d | \* |
| b | a | l | F |
| a | s |  |  |

Ciphertext: pembacaan enkripsi dari kiri atas ke kanan bawah dan karakter spasi berubah menjadi karakter \*

Block decrypt :

Ciphertext : smmbaa\*uaslhdlia\*f (18 karakter)

Menghitung baris tiap kolom yaitu jumlah karakter dibagi 4, jika karakternya fullcoumn 16 maka 16 dibagi 4 adalah 4 baris. Jika karakternya tidak fullcolumn 18 maka 18 mod 4

**Gambar (block encrypt dan ciphertext aplikasi salcrypt)**

**Gambar (ciphertext dan block decrypt aplikasi salcrypt)**

Permutation Encrypt dan Permutation Decrypt

Metode permutation encrypt (permutasian) merupakan metode yang mengacak setiap beberapa karakter dan merubah posisinya. Pada metode ini, pengacakan dibagi dalam setiap 6 karakter. Pada permutation decrypt akan dibalikkan ke posisi semula setiap 6 karakter tersebut.

Contoh:

Plaintext: yodi satriani

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | o | D | i |  | s | a | T | R | i | a | n | i |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| s | o | I | d | \* | y | n | T | I | r | a | a | i |

Ciphertext : soid\*yntiraai

Karakter spasi berubah menjadi karakter \*

Permutation decypher :

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| s | o | I | d | \* | y | n | T | I | r | a | a | i |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | o | D | i |  | s | a | T | r | i | a | n | i |

**Gambar (permutation encrypt dan ciphertext aplikasi salcrypt)**

**Gambar (ciphertext dan permutation decrypt aplikasi salcrypt)**

Expansion Encrypt dan Expansion Decrypt

Metode expansion encrypt merupakan metode dimana karakter pada kata depan dipindahkan ke posisi belakang dan setiap kata ditambahkan huruf akhiran. Pada expansion encrypt ini, setiap karakter pada kata akan dipindahkan ke belakang dan pada akhiran akan ditambahkan huruf “AN” atau “I”. Jika karakter depan pada kata adalah huruf konsonan atau ganjil (b, c, d, f, …, 1, 3, 5, 7, 9) maka akan berakhiran “AN”. Jika karakter depan pada kata adalah huruf vokal atau genap (a, i, u, e, o, 2, 4, 6, 8, 0) maka akan berakhiran “I”.

Contoh :

Plaintext : rafifah oktarinda

Ciphertext : afifahrAN ktarindaoI

Metode expansion decipher adalah metode pengembalian enkripsi dari metode expansion dimana cara kerjanya adalah menyalin setiap kata pada karakter hingga bertemu karakter “A”, “N”, atau “I”, kemudian setiap kata akan dicetak dan ditambahkan spasi. pada karakter “A” akan menyimpan dan menghapus karakter sebelumnya, pada karakter “N” akan memindahkan karakter yang disalin ke depan. Pada karakter I akan menghapus karakter sebelumnya dan menyalin ke depan karakter sebelumnya

Contoh:

Ciphertxet : afifahrAN ktarindaoI

Expansion decrypt :

1. Menyalin “afifahr”
2. Menyalin “afifah” dan menyimpan karakter “r” (bertemu karakter “A”)
3. Menggabungkan karakter yang disimpan dan disalin “r” + “afifah” (bertemu karakter “N”)
4. Disimpan menjadi karakter “rafifah”
5. Pada saat menyalin spasi maka akan dihapus karakter sebelumnya yang disalin (spasi terhapus) dan kemudian menyalin “ktarindao”
6. Menyimpan karakter sebelumnya “o” dan menggabungkan dengan karakter yang disalin “ktarinda” menjadi “oktarinda” (bertemu karakter “I”)
7. Menggabungkan karakter “rafifah” + “ “ + “oktarinda”

Plaintext : rafifah oktarinda

**Gambar (Expansion encrypt dan ciphertext aplikasi salcrypt)**

**Gambar (ciphertext dan expansion decrypt aplikasi salcrypt)**

Compaction Encrypt dan Compaction Decrypt

Metode mengurangi panjang pesan dengan cara menghilangkan setiap karakter ke-n secara berurutan. Karakter-karakter yang hilang akan disatukan kembali dibelakang secara berurutan dan menggunakan karakter khusus. Pada compaction encrypt ini, menghilangkan setiap karakter ke-3 dan menggabungkannya kembali dengan karakter khusus yaitu “&”.

Contoh :

Plaintext : risky parmana putra

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | i | s | K | y |  | p | a | r | m | a | n | a |  | p | u | t | r | a |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | i | k | y | p | a | m | a | a |  | u | t | a | & | s |  | r | n | p | r |

Ciphertext : rikypamaa uta&s rnpr

Setiap karakter ke-3 akan dihilangkan dan digabungkan dibelakang sebagai lampiran bersama karakter khusus “&”

Compaction Decrypt, metode ini mengembalikan hasil enkripsi dari compaction dimana dengan cara mengembalikan karakter dibelakang karakter khusus setiap 2 karakter, dan menghapus karakter khususnya setelah semua karakter dibelakang habis.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | i | k | y | p | a | m | a | a |  | u | t | a | & | s |  | r | n | p | r |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | i | s | k | y |  | p | a | r | m | a | n | a |  | p | u | t | r | a | & |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| r | i | s | k | y |  | p | a | r | m | a | n | a |  | p | u | t | r | a |  |

Hasil compaction decrypt

Plaintext : risky parmana putra

**Gambar (Compaction encrypt dan ciphertext aplikasi salcrypt)**

**Gambar (ciphertext dan Compaction decrypt aplikasi salcrypt)**

**Aplikasi dan Bahasa Pemrograman**

(penjelasan sedikit)

**SARAN**

**DAFTAR PUSTAKA**