NAMA : DON SUBAGIO
MIM :1310651006
KELAS : A

Domain 5: Cryptograph

Tujuan pengujian dalam bab ini

- Konsep corner Stone
- Symetric enskripsi
- Asimetrik enskripsi
- Fungsi hash
- Serangan kriptografi
- Pelaksanaan kriptografi

PENGANTAR

Criptografi adalah penulisan rahasia : komunikasi yang aman yang dapat dipahami oleh penerima saja, dan tidak diketahui oleh pihak ketiga.

KONSEP KRIPTOGRAFI CORNERSTONE

Konsep kriptografi dasar yang diwujudkan oleh semua enkripsi yang kuat dan harus dipahami sebelum belajar tentang implementasi spesifik .

ISTILAH KUNCI

Kriptologi adalah ilmu komunikasi yang aman . Kriptografi menciptakan pesan makna yang tersembunyi ; kriptanalisis adalah ilmu melanggar pesan terenkripsi. kriptologi meliputi Kriptografi dan pembacaan sandi.

Sebuah cipher adalah algoritma kriptografi . Sebuah plaintext adalah pesan terenkripsi . Enkripsi mengubah plaintext ke ciphertext a. Dekripsi ternyata kembali ciphertext menjadi plaintext a.

KERAHASIAAN, INTEGRITAS , OTENTIKASI , dan NONREPUDIATION

Kriptografi dapat memberikan kerahasiaan (rahasia tetap rahasia) dan integritas (data tidak diubah dengan cara yang tidak sah) , penting untuk dicatat Kriptografi juga dapat memberikan otentikasi (membuktikan klaim identitas) .

Substitutisi dan permutasi

Substitusi kriptografi menggantikan satu karakter untuk lain ; ini menyediakan kebingungan. Permutasi (juga disebut transposisi) memberikan difusi dengan mengatur kembali karakter dari plaintext , gaya anagram . " ATTACKATDAWN " dapat diatur kembali untuk " CAAKDTANTATW "

KEKUATAN KRIPTOGRAFI

Enkripsi yang baik adalah yang kuat : untuk enkripsi kunci berbasis , itu harus sangat sulit (dan idealnya tidak mungkin) untuk mengkonversi ciphertext kembali ke plaintext tanpa kunci . faktor pekerjaan menjelaskan berapa lama waktu yang dibutuhkan untuk memecahkan kriptografi (mendekripsi ciphertext a tanpa kunci) .

Kerahasiaan algoritma kriptografi tidak memberikan kekuatan : sebenarnya algoritma rahasia sering terbukti cukup lemah . Kripto kuat bergantung pada perhitungan matematikanya.

MONOALPHABETIC DAN CIPHER POLYALPHABETIC

Sebuah cipher monoalphabetic menggunakan satu huruf : huruf tertentu (seperti " E ") diganti untuk lain (seperti " X ") .

Sebuah cipher polyalphabetic menggunakan beberapa huruf : " E " mungkin digantikan untuk " X " satu putaran dan kemudian " S " babak berikutnya .

NAMA : DON SUBAGIO
MIM :1310651006
KELAS : A

Table 5.1 XOR Truth Table		
X	**Y**	**X XOR Y**
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive Or (XOR)

Exclusive Or (XOR) adalah " rahasia saus " di belakang enkripsi modern. Menggabungkan kunci dengan plaintext melalui XOR menciptakan ciphertext a. XOR - ing untuk kunci yang sama dengan ciphertext mengembalikan plaintext asli . XOR matematika cepat dan sederhana .

Dua bit adalah benar (atau 1) jika satu atau yang lain (eksklusif , tidak keduanya) adalah 1. lainnya kata , jika dua bit berbeda , jawabannya adalah 1 (benar) . Jika dua bit adalah sama, Jawabannya adalah 0 (false) . XOR menggunakan tabel kebenaran , ditunjukkan pada Tabel 5.1 . Ini menentukan bagaimana menggabungkan bit dari kunci dan plaintext .

JENIS KRIPTOGRAFI

Ada tiga jenis utama dari enkripsi yang modern : simetris , asimetris , dan hashing.

1. Enkripsi simetris menggunakan satu kunci: mengenkripsi kunci yang sama dan mendekripsi .
2. Kriptografi asimetris menggunakan dua kunci : jika Anda mengenkripsi dengan satu tombol ,anda mungkin mendekripsikan dengan yang lain.
3. Hashing adalah transformasi kriptografi satu arah menggunakan algoritma (dan tidak ada tombol) .

SYMMETRIC ENCRYPTION

Enkripsi simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi . Jika Anda mengenkripsi file jib dan kemudian mendekripsi dengan kunci yang sama , Anda menggunakan enkripsi simetris . simetris enkripsi juga disebut " kunci rahasia " enkripsi : kunci harus dirahasiakan dari Pihak ketiga.

STREAM DAN BLOK CIPHER

Enkripsi simetris mungkin memiliki aliran dan blok mode . Modus aliran berarti setiap bit secara independen dienkripsi dalam " aliran . " mode Block cipher mengenkripsi blok Data setiap putaran : 56 bit untuk Data Encryption Standard (DES) dan 128 , 192 , atau 256 bit AES , misalnya. Beberapa cipher blok dapat meniru stream cipher oleh pengaturan ukuran blok 1 bit ; mereka masih dianggap cipher blok .

VEKTOR INISIALISASI DAN CHAINING

Vektor inisialisasi digunakan dalam beberapa cipher simetrik untuk memastikan bahwa blok pertama dienkripsi data acak.

Chaining (disebut umpan balik dalam mode aliran) biji dienkripsi sebelumnya blok ke blok berikutnya yang akan dienkripsi .

DES

DES adalah Data Encryption Standard , yang menggambarkan Algoritma Enkripsi data (DEA).

MODE DES

DES dapat menggunakan lima mode yang berbeda untuk mengenkripsi data. Perbedaan utama mode adalah memblokir vs (ditiru) aliran , penggunaan vektor inisialisasi , dan apakah kesalahan di enkripsi akan merambat ke blok berikutnya .

NAMA : DON SUBAGIO
MIM :1310651006
KELAS : A

ASIMMETRIK ENSKRIPSI

Enkripsi asimetris menggunakan dua kunci : jika Anda mengenkripsi dengan satu tombol , Anda dapat mendekripsi dengan lainnya . Salah satu kunci dapat dibuat publik (disebut kunci publik) ; asimetris enkripsi juga disebut enkripsi kunci publik untuk alasan ini . Siapa pun yang ingin untuk berkomunikasi dengan Anda mungkin cukup download kunci publik Anda diposting publik dan menggunakannya untuk mengenkripsi plaintext mereka . Setelah dienkripsi , kunci publik Anda tidak dapat mendekripsi plaintext : hanya kunci pribadi Anda dapat melakukannya . Seperti namanya , kunci pribadi Anda harus dirahasiakan dan aman .

BAGIAN-BAGIAN ASIMETRIS ENSKRIPSI ADALAH :

1. Metode Asymmetric
2. Pemfaktoran bilngan prima
3. logaritma diskrit

FUNGSI HASH

Sebuah fungsi hash memberikan enkripsi menggunakan algoritma dan tidak ada tombol . Mereka disebut " Fungsi hash satu arah " karena tidak ada cara untuk membalikkan enkripsi . SEBUAH variabel - panjang plaintext " hash " menjadi (biasanya) tetap-panjang nilai hash (sering disebut " message digest " atau hanya " hash ") . Fungsi hash terutama digunakan untuk menyediakan integritas : jika hash dari perubahan plaintext , plaintext sendiri telah berubah . Fungsi hash yang lebih tua umum termasuk Secure Hash Algorithm 1 (SHA - 1) , yang menciptakan hash 160 - bit dan Message Digest 5 (MD5) , yang menciptakan hash 128 - bit . Kelemahan telah ditemukan di kedua MD5 dan SHA - 1 ; alternatif baru seperti sebagai SHA - 2 yang direkomendasikan .

SERANGAN KRIPTOGRAFI

Serangan kriptografi digunakan oleh cryptanalysts untuk memulihkan plaintext tanpa kunci. Harap diingat bahwa pemulihan kunci (kadang-kadang disebut " mencuri kunci ") adalah biasanya lebih mudah daripada melanggar enkripsi modern. Ini adalah apa penegak hukum biasanya tidak ketika berhadapan dengan tersangka menggunakan kriptografi : mereka mendapatkan surat perintah pencarian dan mencoba untuk memulihkan kunci, contoh serangan kriptografi antara lain :

1. Brute Force
2. Known plaintext
3. Chosen plaintext and adaptive-chosen plaintext
4. Chosen ciphertext and adaptive-chosen ciphertext
5. Meet-in-the-middle attack
6. Known Key
7. Differential cryptanalysis
8. Linear cryptanalysis
9. Side-channel attacks

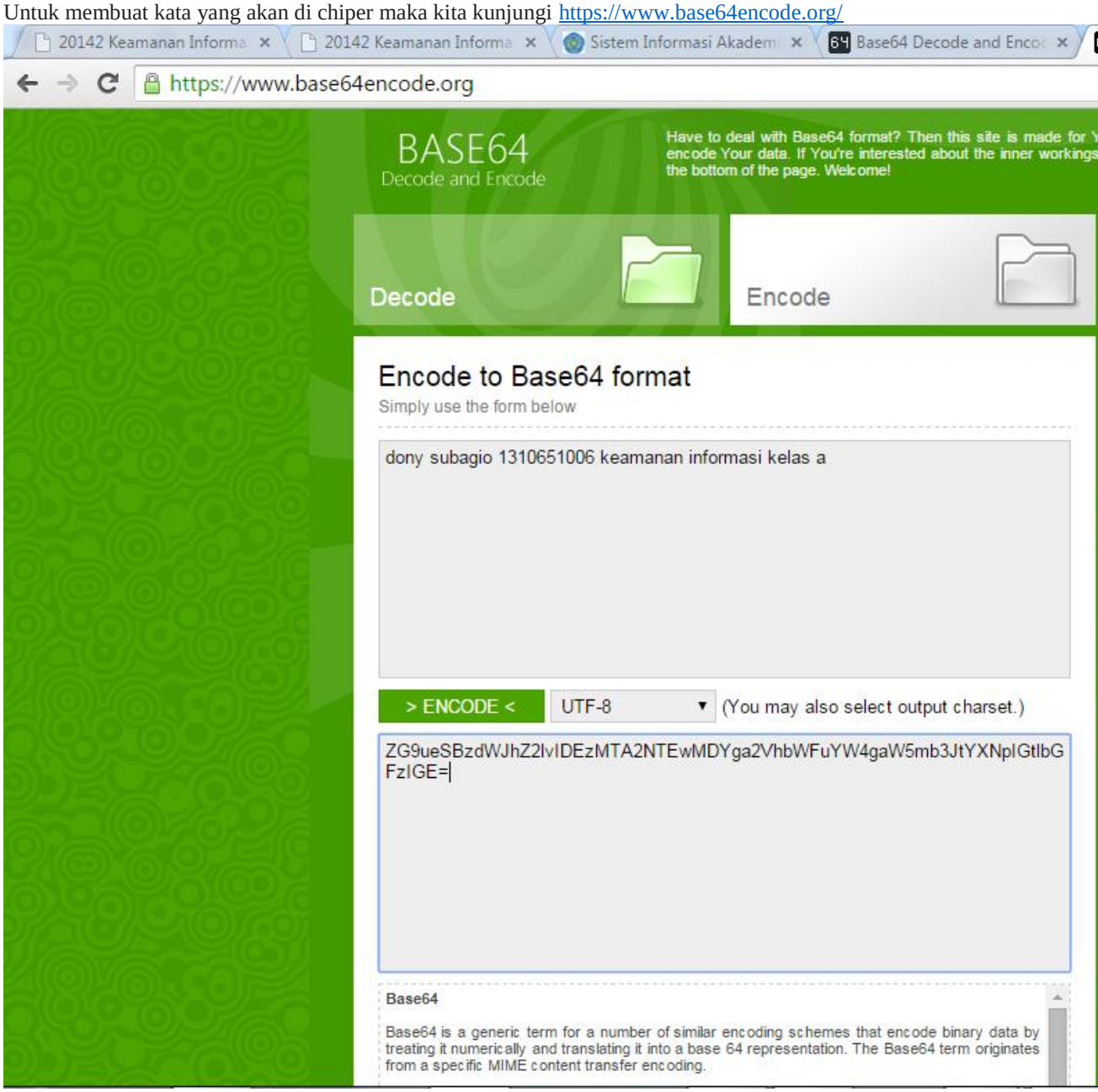
NAMA : DON SUBAGIO
MIM :1310651006
KELAS : A

CONTOH KASUS KRIPTOGRAFI : Base64 format

Di sini saya akan menjelaskan tentang pembuatan kriptografi menggunakan base64 format.
Cara yang akan saya gunakan adalah base64 versi Online atau masuk pada alamat
https://www.base64decode.org/

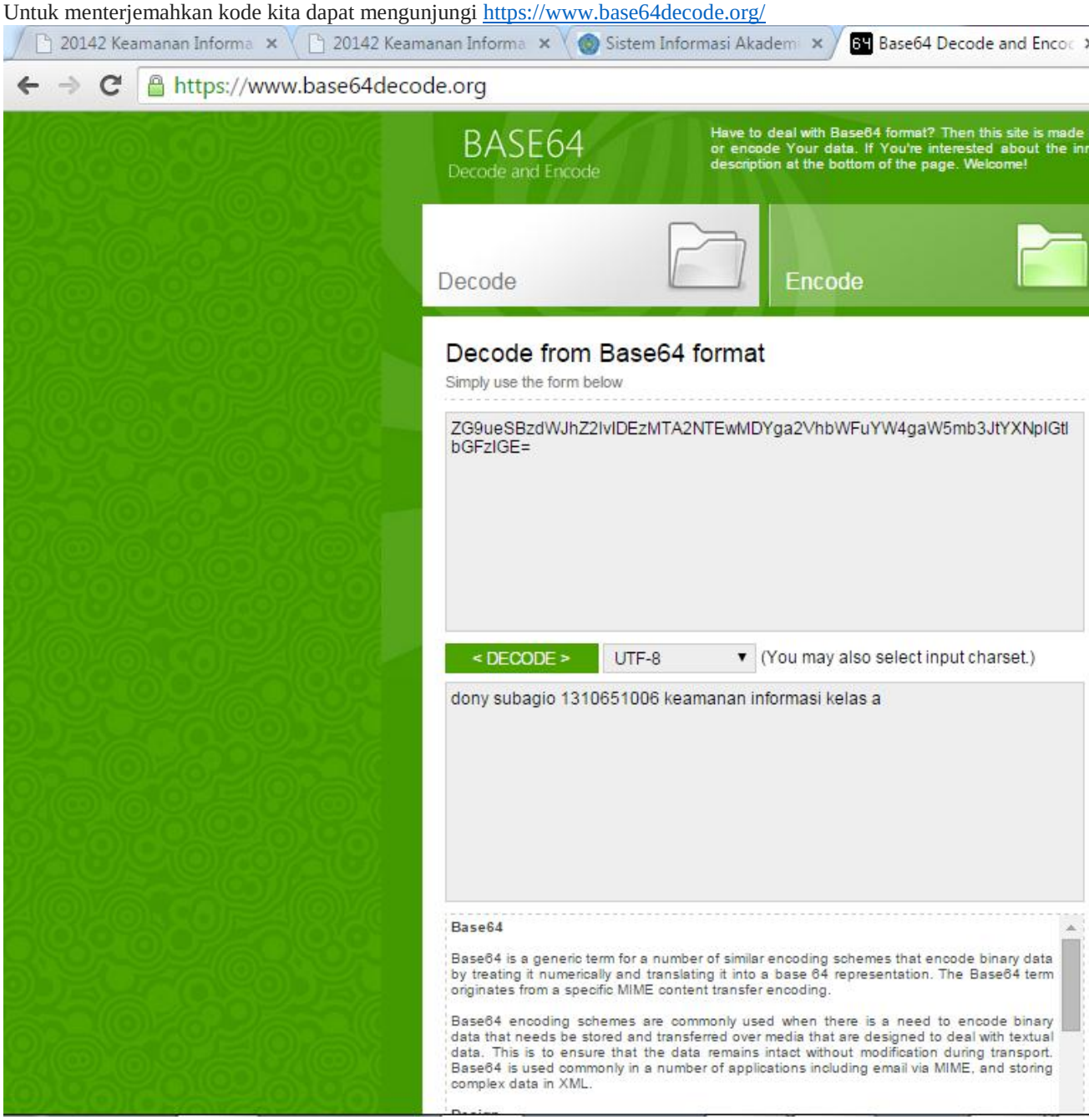
langkah-langkah :

1. Pastikan memiliki koneksi internet.
2. Buka browser anda
3. Untuk membuat kata yang akan di chiper maka kita kunjungi https://www.base64encode.org/



NAMA : DON SUBAGIO
MIM :1310651006
KELAS : A

4. Untuk menterjemahkan kode kita dapat mengunjungi https://www.base64decode.org/



Semoa artikel di atas dapat berguna bagi kita semua , dan di mohon dengan sangat , agar menggunakan pengetahuan anda , untuk hal-hal yang positif , serta tidak merugikan orang lain.