PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL

M O D U L 1
P R A T I K U M

CRYPTOGRAPHY

PENYUSUN

AGUNG MULYO WIDODO,ST. ,MSc.
Drs. HOLDER SIMORANGKIR, MT.

MENGETAHUI
KEPALA PROGRAM STUDI

BAMBANG IRAWAN, S.Kom, M.Kom

PRATIKUM 1

CAESAR CIPHER

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep cryptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Algoritma kriptografi klasik:

   - *Cipher* Substitusi (*Substitution Ciphers*)
   - *Cipher* Transposisi (*Transposition Ciphers*)

   Teknik Subtitusi

   Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak. Contoh : Tabel subsitusi Caesar Chipher, ROT 13. Chiper subtitusi di bedakan sebagai berikut :

   Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext.

   Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext.

   Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext

Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext.

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :

   - Buatlah tabel subtitusi berikut :

   A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.-,

   B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

   Pada baris pertama adalah plaintext dan baris kedua adalah chiper.

   - Buatlah chiper dari plaintext berikut :

   Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data, atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan, tanpa memerlukan kuncinya.

   - Buatlah plaintext tersebut degan menggunakan teknik Caesar Chiper. Bandingkan.

5. Buatlah kesimpulan.

PRATIKUM 2

VIGÈNERE CIPHER

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Algoritma kriptografi klasik:

   - *Cipher* Substitusi (*Substitution Ciphers*)
   - *Cipher* Transposisi (*Transposition Ciphers*)

   Teknik Subtitusi

   Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak. Contoh : Tabel subsitusi Caesar Chipher, ROT 13. Chiper subtitusi di bedakan sebagai berikut :

   Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext.

   Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext.

   Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext

Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext.

Vigènere Cipher termasuk ke dalam cipher abjad-majemuk (**polyalpabetic substitution cipher**). Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan **Vigènere Cipher**.

Vigènere Cipher menggunakan **Bujursangkar Vigènere** untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher.

3. Bahan dan peralatan

Bahan yang di perlukan dalam pratikum ini adalah :

- Alat tulis dan kertas

4. Langkah-langkah percobaan :

- Buatlah **Bujursangkar Vigèner** berikut :

Kunci \ Plainteks	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 4.2 Bujursangkar *Vigènere*

- Buatlah chiper dari plaintext berikut :

Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan

ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya

- Buatlah plaintext tersebut dengan menggunakan kunci : **sony**
- Buatlah kesimpulan.

PRATIKUM 3

ROT 13 CIPHER

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Algoritma kriptografi klasik:

   - *Cipher* Substitusi (*Substitution Ciphers*)
   - *Cipher* Transposisi (*Transposition Ciphers*)

   Teknik Subtitusi

   Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak. Contoh : Tabel subsitusi Caesar Chipher, ROT 13. Chiper subtitusi di bedakan sebagai berikut :

   Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext.

   Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext.

   Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext

Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext.

Pada sistem **ROT13** sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai:

$$C\ ROT13 = (M)$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali.

$$M = ROT13(ROT13(M))$$

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :

   - Buatlah **tabel ROT13** dari karakter-karakter berikut :

   A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.-,

   - Buatlah chiper dengan menggunakan tabel ROT13 dari plaintext berikut :

   Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya

   - Buatlah kesimpulan.

PRATIKUM 4

TEKNIK BLOCKING

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Teknik Blocking

   Blocking adalah sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen. Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini. Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya.

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :
   - Buatlah chiper dengan menggunakan teknik blocking dengan **1 blok berisi 4 karakter** dari plaintext berikut :

   Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya
   - Buatlah kesimpulan.

PRATIKUM 5

TEKNIK PERMUTASI

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Teknik Permutasi/ Transposisi

   Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi.

   Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.

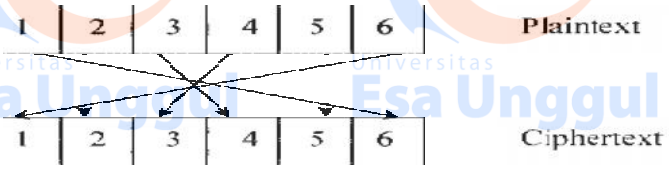
   Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :
   - Buatlah chiper dengan menggunakan teknik permutasi dengan **membagi plaintext menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :**



   - Plaintext sebagai berikut :

   Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya
   - Buatlah kesimpulan.

PRATIKUM 6

TEKNIK EKSPANSI

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Teknik Ekspansi

   Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i"

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :

   - Buatlah chiper dengan menggunakan teknik ekspansi plaintext sebagai berikut :

Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya

- Buatlah kesimpulan.

PRATIKUM 7

TEKNIK PEMAMPATAN

1. **Tujuan :**

   Mahasiswa mengerti dan memahami konsep crptography klasik dengan menggunakan teknik-teknik dasar cryptography.

2. **Teori :**

   Teknik dasar cryptography terdiri dari :

   - Substitusi
   - Blocking
   - Permutasi
   - Ekspansi
   - Pemampatan

   Algoritma kriptografi klasik berbasis karakter dengan menggunakan pena dan kertas saja, belum menggunakan computer. Termasuk ke dalam kriptografi kunci-simetri

   Teknik Pemampatan

   Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan.

   Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&".

3. Bahan dan peralatan

   Bahan yang di perlukan dalam pratikum ini adalah :

   - Alat tulis dan kertas

4. Langkah-langkah percobaan :

   - Buatlah chiper dengan menggunakan teknik pemampatan, plaintext sebagai berikut :

   Seorang penyerang bisa menemukan kunci dan dengan demikian memiliki kunci untuk mendekripsi semua blok data atau seorang penyerang bisa mengumpulkan ciphertext dan plaintext dari masing-masing blok dan membangun buku kode yang digunakan tanpa memerlukan kuncinya

   - Buatlah kesimpulan.

Referensi :

1. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
2. HCA van tilborg, " Fundamentals of cryptography", Kluwer academic publisher.
3. C. Paar,J.Pelzl,"Understanding Cryptography-Textbook for Student and Practitioners", 2009