PEMAHAMAN KRIPTOGRAFI SUPER ENKRIPSI

Maradu Sihombing
(Dosen Akademi Manajemen Informatika Komputer
Medan Bussiness Polytechnic Medan)

ABSTRAK

Kriptografi merupakan suatu teknik untuk merahasiakan sesuatu (tulisan, suara, angka, dan lain lain) ke bentuk yang tidak dimengerti oleh orang awan, hanya orang tertentu yang mengerti. Hal super enkripsi sangat sedikit dibahas pada buku, tidak ada sampai mendetail. Untuk itu, makalah ini membahas metode super enkripsi yang merupakan satu diantara metoda kriptografi klasik yang menerapkan cipher subsitusi dan cipher transposisi dikombinasikan untuk menghasilkan cipher yang lebih kuat (super), sedangkan metode lain hanya satu cipher saja. Plainteks dienkripsi dengan cipher transposisi, lalu hasilnya (ciphertext) dienkripsikan lagi dengan cipher subsitusi Caesar Cipher (atau dapat juga sebaliknya). Dengan dibuatnya makalah ini, maka pemahaman kriptografi super enkripsi menjadi mudah dipahami konsep kerjanya.

Kata kunci : Kriptografi, subsitusi, transposisi, plainteks, cipherteks, privacy, super enkripsi

1. PENDAHULUAN

Kriptografi berasal dari bahasa Yunani “criptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Jadi kriptografi berarti tulisan rahasia. Defenisi kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Sejarah kriptografi menurut David Kahn yang berjudul “The codebreakers”, telah digunakan oleh bangsa Mesir 4000 tahun lalu, berupa hieroglyph yang tidak standard pada pyramid. Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi yang ingin kerahasiaan dalam komunikasi pesan pentingnya. Mereka itu adalah kalangan militer (khususnya intelijen atau mata-mata), kalangan diplomatik, penulis buku harian, dan kalangan pecinta (lovers). Dewasa ini pemakaian komputer sudah diterapkan dalam berbagai bidang, misalnya transaksi pada ATM, percakapan dengan video conference, pendaftaran mahasiswa online, transaksi pengisian pulsa, pengisian KRS, ujian kompetensi online, pengiriman nilai. Semua hal tersebut dilakukan karena sudah merasa aman dari gangguan (atau pengganggu). Untuk itu sangat diperlukan kriptografi untuk keamanan informasi (information security), sehingga keamanan informasi tidak bisa dipisahkan dengan kriptografi. Penggunaan kriptografi sudah sering dipakai dalam kehidupan sehari-hari, misalnya pemasukan pin ATM ditekan kombinasi bilangan 0,1,2,3,4,5,6,7,8,9 yang ditampilkan hanya tanda bintang (*) sebanyak angka yang ditekan, begitu juga jika memasukkan password ke komputer, atau saat membuka

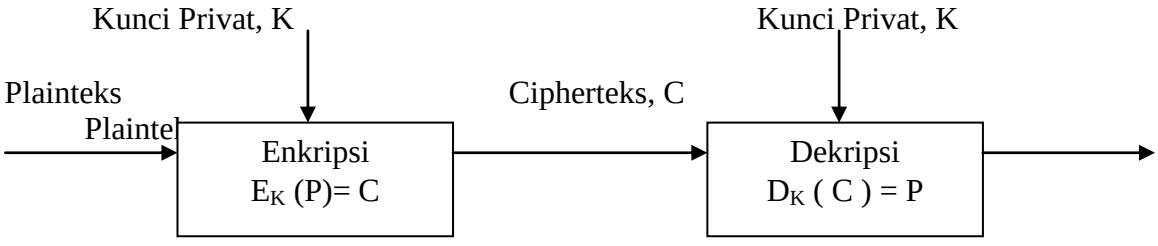
email, semua yang ditekan dari keyboard ditampilkan ke bentuk * sebanyak tompol yang ditekan.

Untuk menyatakan keamanan, harus ditinjau dari beberapa hal yaitu kerahasiaan (privacy), integritas data (data integrity), otentikasi (authentication), ketidakbenaran penyangkalan (non-repudiation). Dalam mempelajari kriptografi ada terminology (istilah) yang penting diketahui yaitu (1) Pesan, Plainteks, dan Cipherteks, yaitu yang berhubungan dengan pesan atau plainteks (message = data atau informasi yang dibaca dan dimengerti maknanya). Sedangkan cipherteks adalah pesan yang sudah tersandikan sehingga tidak dapat dipahami lagi maknanya. (2) Sender dan receiver (Pengirim, Penerima). (3) Enkripsi dan dekripsi. Proses penyandian plainteks menjadi cipherteks disebut enkripsi, sedangkan proses pengembalian cipherteks ke bentuk aslinya disebut dekripsi. (4) Cipher dan kunci. Cipher disebut juga fungsi matematika yang digunakan untuk enkripsi dan dekripsi, konsep matematika yang mendasarinya adalah relasi antara dua buah himpunan elemen plainteks dengan himpunan elemen cipherteks.

2. METODELOGI

Berdasarkan sejarah kriptografi, maka kriptografi dibedakan menjadi kriptografi klasik dan kriptografi modern. Sedangkan berdasarkan kunci yang digunakan untuk enkripsi atau dekripsi, maka kriptografi dapat dibedakan menjadi kriptografi kunci simetris dan kriptografi kunci a-simetris. Kriptografi klasik masih berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan, yang juga termasuk ke kriptrografi simetris. Kriptografi klasik perlu dipelajari karena : (1) dapat memberikan pemahaman konsep dasar kriptografi. (2) sebagai dasar kriptografi modern. (3) untuk memahami potensi-potensi kelemahan cipher. Pada dasarnya algoritma kriptografi klasik dikelompokkan menjadi dua cipher yaitu cipher substitusi, dan cipher transposisi. Metode yang tergolong pada substitusi yaitu Caesar Cipher, Cipher Alfabet Tunggal, Cipher Alfabet Majemuk, Cipher Homofonik, dan Cipher Poligram.

Pada kriptografi kunci simetris, dimana kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi, seperti gambar di bawah ini.

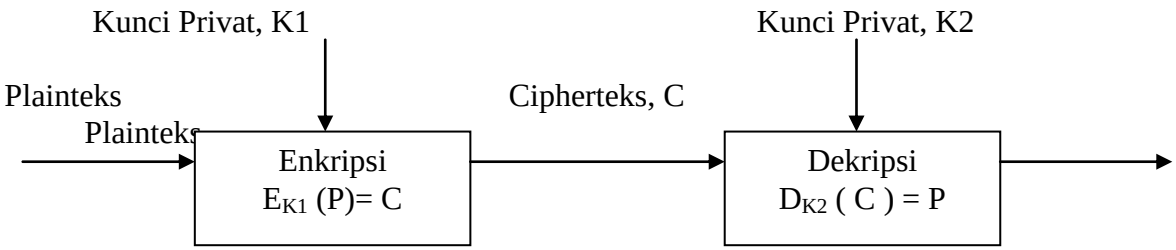


Gambar 1. Skema kriptografi simetris, kunci enkripsi dan dekripsi sama yaitu K

Algoritma modern yang tergolong ke kriptografi klasik ini yaitu DES, Blowfish, Twofis, Triple-DES, IDEA, Serpent, juga AES. Jika kunci untuk proses enkripsi dan dekripsi tidak sama, maka disebut kriptografi A-simetris, disebut juga kriptografi kunci-publik, sebab kunci untuk enkripsi tidak dirahasiakan, tapi

kunci dekripsinya harus dirahasiakan. Contoh algoritma kriptografi modern yang tergolong ke dalamnya yaitu RSA, Elgamal, DSA.

Pada kriptografi kunci a-simetris, dapat digambarkan seperti gambar di bawah ini.



Gambar 2. Skema kriptografi a-simetris, kunci enkripsi K1 dan dekripsi K2

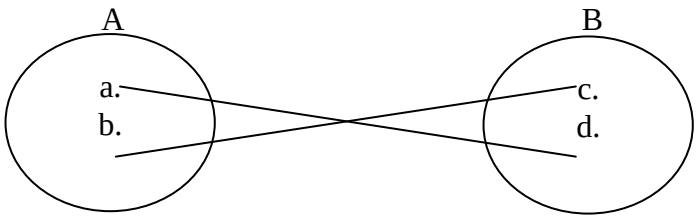
Untuk mempelajari kunci, sering dihubungkan dengan fungsi, permutasi dan kombinasi, peluang, dan bilangan. Matematika yang diperlukan untuk kriptografi adalah matematika diskrit.

Fungsi

Dalam matematika, himpunan A dan B dapat direlasikan dengan fungsi f, dimana setiap elemen di A dihubungkan dengan tepat satu elemen di B, dapat dituliskan sebagai berikut :

$f : A \rightarrow B$ 1

Nama lain untuk fungsi adalah pemetaan atau transformasi. ***f(a)*** = b jika elemen a di dalam A dihubungkan dengan elemen b di dalam B. Himpunan A disebut domain (asal) dari f dan himpunan B disebut daerah hasil (codomain) dari f.



Gambar 3 Fungsi f memetakan A ke B.

Permutasi dan Kombinasi

Permutasi adalah jumlah urutan berbeda dari pengaturan obyek-obyek. Permutasi dari n obyek adalah

$n(n-1)(n-2) \ldots .(2)(1) = n!$ 2

dari persamaan di atas (2) dapat disimpulkan permutasi ekivalen dengan faktorial n. Jika permutasi ***r*** dari ***n*** obyek, dapat disimbolkan ***P(n,r)*** dengan ketentuan $r \leq n$, dinyatakan dengan persamaan berikut:

$$P(n, r) = \frac{n!}{(n-r)!} \quad \ldots \quad 3$$

Bentuk permutasi persamaan (2) dapat dirubah ke kombinasi. Kombinasi r elemen dari n elemen dapat disimbolkan menjadi C (n, r) dengan persamaan sebagai berikut:

$$C(n, r) = \frac{n!}{r!\,(n-r)!} \quad \ldots \quad 4$$

Teori Informasi

Teori ini pertama sekali dipopulerkan oleh Shannon pada tahun 1984, yang mendefenisikan jumlah informasi di dalam pesan sebagai jumlah minimum bit yang dibutuhkan untuk mengkodekan pesan. Misalnya 1 bit untuk mengkodekan jenis kelamin (1=laki-laki, 0 = perempuan), 4 bit untuk mengkodekan 0 s/d 9 (0 = 0000, 1 = 0001, 7 = 0111, 9 = 1001), 3 bit untuk mengkodekan nama hari (minggu = 000, senin = 001, selasa = 010, sabtu = 111), hal ini yang disebut dengan entropi yang dapat dirumuskan dengan persamaan.

$$H(X) = -\sum_{i=1}^{n} pi\ log2\ (pi) \quad \ldots \quad 5$$

Dengan ketentuan X = pesan, n = jumlah simbol berbeda di dalam pesan, dan p_i = peluang kemunculan simbol ke-i.

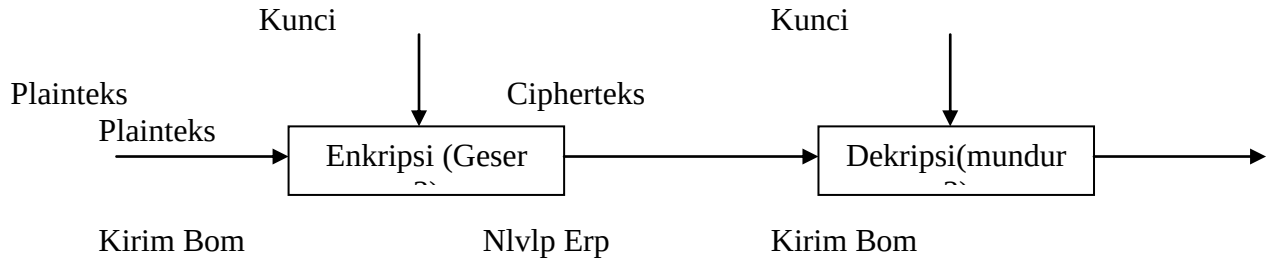
Teori Bilangan

Bilangan yang dimaksudkan adalah bilangan bulat integer. Teori bilangan relatif prima dapat dijelaskan dua buah bilangan bulat a dan b dikatakan relatif prima jika pembagi bersama terbesar (PBB) dari (a, b) =1. Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga ***ma* + *nb* =1**. Aritmatika modulo adalah bilangan bulat ***m*** yang lebih besar dari 0 dibagi dengan bilangan bulat ***n*** yang juga lebih besar dari 0 memberikan sisa, yang juga bilangan bulat ***l*** yang mempunyai nilai antara 0,1,2,3 .. ***m-1***. Dengan demikian dapat dituliskan menjadi **m *mod* n = l** sehingga **m = nr + l**, dengan **0 ≤ l ≤ m**, dan r adalah hasil bagi. Bila harga m bernilai negatif, harus diabsolutkan.

3. PEMBAHASAN

Untuk mempelajari makalah ini, akan dijalankan dasar-dasar **Caesar Cipher** yang berhubungan dengan kriptografi yaitu skema enkripsi dan dekripsi, serta illustrasi enkripsi dan dekripsi suatu pesan.

Gambar 4. Skema enkripsi dan dekripsi



Gambar 5. Contoh ilustrasi enkripsi dan dekripsi dengan pesan "Kirim Bom".

Dari gambar 5 di atas pesan / plainteks "Kirim Bom" akan dirahasiakan dengan metode geser 3, maka didapat hasilnya (cipherteks) "NlvlpErp". Dan bila cipherteks tersebut didekripsikan dengan metode mundur 3, maka dihasilnya "Kirim Bom". Dengan demikian kunci yang dipakai pada proses enkripsi adalah **cipher subsitusi yaitu geser 3**. Sedangkan kunci pada proses dekripsi juga **cipher subsitusi yaitu mundur 3**. Sebagai panduan dapat dilihat tabel dibawah ini.

Tabel 1. Tabel subsitusi dengan geser 3.

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
Cipherteks	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

Bila setiap alphabet dengan integer (A = 0, B =1, C= 2,…., Z=25), maka secara matematika pergeseran 3 huruf alphabet ekivalen dengan melakukan operasi modulo terhadap P (Plainteks) menjadi C (Cipherteks) dengan persamaan berikut:

$C = E(P) = (P + 3) \bmod 26$ ………………………………………… 6

Sedangkan untuk proses dekripsi (Cipherteks menjadi Plainteks) dinyatakan dengan persamaan berikut ini.

$P = D(P) = (C – 3) \bmod 26$ ………………………………………… 7

Secara umum, untuk pergeseran huruf sejauh k (k adalah kunci enkripsi, dekripsi, dan nilai $k \neq 0$ atau $k \neq 26$), fungsi enkripsinya dengan persamaan

$C = E(P) = (P + k) \bmod 26$ …………………………..………… 8

Dan fungsi dekripsi adalah

$P = D(C) = (P - k) \bmod 26$ ……………………………………… 9

Cipherteks yang dihasilkan harus dirubah menjadi kelompok-kelompok yang terdiri dari beberapa huruf, hal ini dilakukan agar kriptanalis lebih susah memecahkan cipherteks tesebut.

Contoh :

Plainteks	SEMUT DAN KANCIL HEWAN CERDAS
Cipher (asli)	VHPXW GDQ NDQFLO KHZDQ FHUGDV
Cipher (dikelompokan 5)	VHPXW GDQND QFLOK HZDQF HUGDV

Cipher Transposisi, pesan yang akan dienkripsikan hanya urutannya yang dirubah, sehingga hanya melakukan algoritma transpose terhadap pesan tersebut. Dengan demikian metode ini disebut juga permutasi atau pengacakan pada pesan.

Contoh :

Plainteks	SEMUT DAN KANCIL HEWAN CERDAS
Cipher (lebar 5)	S E M U T D A N K A N C I L H E W A N C E R D A S
Cipher (baca vertical)	SDNEEEACWRMNIADUKLNATAHCS
Cipher (dikelompokan 5)	***SDNEE EACWR MNIAD UKLNA TAHCS***

Dalam makalah ini yang diterapkan super enkripsi (**Cipher Transposisi** dan **Caesar Cipher**), maka didapat hasil yang sangat susah dipecahkan. Misalnya :

Metode	Plainteks	SEMUT DAN KANCIL HEWAN CERDAS
T R A N S P O S I S	Cipher (lebar 5) (perkatikan 5 baris, **5 kolom**) Cipher (baca	↓ **S E M U T** **D A N K A** **N C I L H** **E W A N C** **E R D A S** SDNEEEACWRMNIADUKLNATAHCS

I	vertical) Cipher (kelompok 5)	SDNEE EACWR MNIAD UKLNA TAHCS
Metode	Plainteks	SDNEE EACWR MNIAD UKLNA TAHCS
C A E S A R	Cipherteks (Geser 3) A →D, B → E,… Z →C Ciphertkes (kelompok 3)	VGQHH HDFZU PQLDG XNOQD WDKFV **VGQ HHH DFZ UPQ LDG XNO QDW DKFV**
Hasil	**Cipherteksnya**	**VGQ HHH DFZ UPQ LDG XNO QDW DKFV**

Dari contoh tersebut diperoleh plainteks SEMUT DAN KANCIL HEWAN CERDAS, dienkripsi dengan metode super enkripsi yang dimakalah ini dihasilkan cipherteks **VGQ HHH DFZ UPQ LDG XNO QDW DKFV**.

Bila dilakukan proses dekripsi untuk menghasilkan plainteks asli, dapat dilakukan dengan contoh dibawah ini.

Metode	Cipherteks (kelompok3)	**VGQ HHH DFZ UPQ LDG XNO QDW DKFV**
C A E S A R	Ciphertkes (kelompok 5) Cipherteks (mundur 3) A ←D, B ← E,… Z ←C	VGQHH HDFZU PQLDG XNOQD WDKFV SDNEE EACWR MNIAD UKLNA TAHCS
Metode	Cipherteks (hasil **Caesar**)	SDNEE EACWR MNIAD UKLNA TAHCS
T R A N S P O S I S I	Cipher (lebar 5) (perkatikan **5 baris**, 5 kolom) Cipher (baca vertical)	**SDNEE** **EACWR** **MNIAD** **UKLNA** **TAHCS** SEMUTDANKANCILHEWANCERDAS SEMUT DANKA NCILH EWANC ERDAS

	Cipher (kelompok 5)	
Hasil	Plainteks(Tebak)	SEMUT DAN KANCIL HEWAN CERDAS

Algoritma untuk enkripsi dipakai:

1. Baca plainteks
2. Tuliskan plainteksnya secara horizontal dengan **lebar kolom L** tetap **(L≠1 atau L≠ Panjang plainteks).**
3. Baca dan tuliskan secara vertikal.
4. Tuliskan lagi dengan kelompok-kelompok yang terdiri dari beberapa huruf **(tidak boleh 1 atau sama dengan panjang plainteks).** Dan ini merupakan **Cipherteks** (hasil dari transposisi).
5. Baca Cipherteks (cipherteks ini adalah plainteks untuk metode Caesar Cipher)
6. Buat tabel Caesar dengan pergesaran yang diinginkan (geser ≠ 1 atau geser ≠ 26).
7. Substitusikan Plainteks dengan tabel yang terbentuk
8. Tuliskan hasilnya dengan kelompok-kelompok yang tetap dan hasilnya sudah merupakan ciphertext.
9. Selesai

Bagan dari algoritma enkripsi tersebut di atas:

Nomor langkah	Prosesnya
1.	KERUSUHAN KOTA MEDAN HARUS DIAWASI
2. (L = 10) Baris 3, **kolom 10**	KERUSUHANK OTAMEDANHA RUSD I AWAS I
3.	KORETURASUMDSEIUDAHAWANANHSKAI
4. (kelompok 5)	***KORET URASU MDSEI UDAHA WANAN HSKAI***
5. Cipherteks = Plainteks	KORET URASU MDSEI UDAHA WANAN HSKAI
6. Gesar = 6 A →G, B →H, …, Z →F	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 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
7. K→Q	QUXKZ AXGYA SJYKO AJGNG CGTGT NYQGO
8. kelompok 6 ***Cipherteks***	***QUXKZA XGYASJ YKOAJG NGCGTG TNYQGO***

Bila Ciphertks : QUXKZA XGYASJ YKOAJG NGCGTG TNYQGO dicari plainteksnya, Kemungkinan dari kunci yang ada dan bila hanya dipakai Caesar Cipher.

Nomor	**Cipherteks**					Geser A menjadi
	QUXKZA	XGYASJ	YKOAJG	NGCGTG	TNYQGO	
1	RVYLAB	YHZBTK	ZLPBKH	OHDHUH	UOZRHP	B
2	SWZMBC	Z IACUL	AMQCLI	P I E I V I	VPASIQ	C
3	TXANCD	AJBDVM	BNRDMJ	QJ F J WJ	WQBTJR	D
4	UYBODE	BKCEWN	COSENK	RKGKXK	XRCUKS	E
5	VZCP EF	CLDFXO	DPTFOL	SL HLYL	YSDVLT	F
6	WADQFG	DMEGYP	EQUGPM	TMIMZM	ZTEWMU	G
7	XBERGH	ENFHZQ	FRVHQN	UNJNAN	AUFXNV	H
8	YCFSH I	FOGIAR	GSWIRO	VOKOBO	BVGYOW	I
9	ZDGT I J	GPHJBS	HTXJSP	WPLPCP	CWHZPX	J
10	AEHUJK	HQIKCT	IUYKTQ	XQMQDQ	DXIAQY	K
11	BF I VKL	IRJLDU	JVZLUR	YRNRER	EYJBRZ	L
12	CGJWLM	JSKMEV	KWAMSV	ZSOSFS	FZKCSA	M
13	DHKXMN	KTLNFW	LXBNWT	ATPTGT	GALDTB	N
14	E I LYNO	LUMOGX	MYCOXU	BUQUHU	HBMEUC	O
15	F JMZOP	MVNPHY	NZDPYV	CVRVIV	ICNFVD	P
16	GKNAPQ	NWOQIZ	OAEQZW	DWSWJW	JDOGWE	Q
17	HLOBQR	OXPRJA	PBFRAX	EXTXKX	KEPHXF	R
18	I MPCRS	PYQSKB	QCGSBY	FYUYLY	LFQIYG	S
19	JNQDST	QZRTLC	RDHTCZ	GZVZMZ	MGRJZH	T
20	**KORETU**	**RASUMD**	**SEIUDA**	**HAWANA**	**NHSKAI**	***U***
21	L PSFU V	SBTVN E	TFJVEB	IBXBOB	OITLBJ	V
22	MQTGVW	TCUWOF	UGKWFC	JCYCPC	PJUMCK	W
23	NRUHWX	UDVXPG	VHLXGD	KDZDQD	QKVNDL	X
24	OSV I XY	VEWYQH	WIMYHE	LEAERE	RLWOEM	Y
25	PTWJ YZ	WFXZ R I	XJNZIF	MFBFSF	SMXPFN	Z

Bila diambil dari kemungkinan kunci yang dihasilkan diatas, tidak ada yang cocok.

Algoritma untuk dekripsi dipakai:

1. Baca cipherteks
2. Buat tabel Caesar dengan pergesaran mundur yang diinginkan (geser ≠ 1 atau geser ≠ 26)
3. Substitusikan Cipherteks dengan tabel yang terbentuk
4. Tuliskan cipherteks dengan kelompok yang diinginkan.
5. Tuliskan Cipherteks (cipherteks ini adalah plainteks untuk metode Transposisi)
6. Tuliskan plainteksnya secara horizontal dengan **lebar baris L** tetap pada saat enkripsi **(L≠1 atau L≠ Panjang plainteks).**
7. Baca dan tuliskan secara vertikal.
8. Tuliskan lagi dengan kelompok-kelompok yang mendekati plainteks yang mungkin. Dan ini merupakan **Plainteks** (hasil dari transposisi).
9. **Selesai**

Bagan dari algoritma dekripsi tersebut di atas:

Nomor langkah	Prosesnya
1.	***QUXKZA XGYASJ YKOAJG NGCGTG TNYQGO***
2. Gesar	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

mundur = 6 A←G, B ←H, …, Z ←F	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
3.	KORETU RASUMD SEIUDA IAWANA NHSKAI
4. Kelomok= 5	KORET URASU MDSEI UDAIA WANAN HSKAI
5. Cipherteks = Plainteks	***KORET URASU MDSEI UDAIA WANAN HSKAI***
6. lebar=3 (Lihat saat Enkripsi **baris 3**, kolom 10)	KOR ET U RAS UMD S E I UDA HAW ANA NH S K A I
7.	KERUSUHANKOTAMEDANHARUSDIAWASI
8. **Plainteks** Hasil	***KERUSUHAN KOTA MEDAN HARUS DIAWASI***

4. KESIMPULAN

Kriptografi sangat diperlukan dalam dunia komputer, khususnya untuk merahasiakan suatu pesan yang dijaga kerahasiaannya, misalnya surat-surat rahasia Negara, Ijazah. Kriptografi Super Enkripsi, seperti yang dibahas dalam makalah ini sudah dapat menjadi menjamin kerahasiaan karena sangat susah dipecahkan plainteksnya dibandingkan metode lain. Dengan adanya makalah ini, sudah dapat mempermudah pembaca untuk memahami konsep kerja kriptografi super enkripsi, juga hendaknya diujicoba dengan dalam pengiriman E-mail.

DAFTAR PUSTAKA

Munir Rinaldi, ***Kriptografi***, Penerbit Infomatika, Bandung, 2006.

Sadikin Rifki, ***Kriptografi Untuk Keamanan Jaringan***, Penerbit Andi, Yogyakarta, 2012.

Ariyus Dony, ***Computer Security***, Penerbit Andi, Yogyakarta, 2006.

Ariyus Dony & Andri Rum K.R***, Komunikasi Data***, Penerbit Andi, Yogyakarta, 2008.