ANALISIS PERBANDINGAN KEAMANAN KRIPTOGRAFI KLASIK PADA ALGORITMA SECURE HILL CIPHER BERBASIS KODE ASCII DAN MONOALPHABETIC

Rasudin, Zulfan, Pobi Rizki

Jurusan Informatika Universitas Syiah Kuala

rasudin@unsyiah.ac.id

Abstrak

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data,pesan dan informasi. Pengirim suatu pesan, data dan informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi. Kriptografi merupakan sebuah ilmu yang mempelajari tentang proses pengamanan data. *Secure Hill Cipher* merupakan algoritma modifikasi dari algoritma *Hill* Cipher yang ditemukan pada tahun 1929 oleh L.S. Hill yang merupakan algoritma kriptografi klasik simetris yang sangat terkenal berbasis transformasi matriks. Tujuan dari penelitian ini adalah untuk dapat melihat perbandingan kemanan dari pada algoritma modifikasi *Secure Hill Cipher* berbasis kode ASCII dan *MonoAlphabetic*. Pada hasil analisa menggunakan tool SPSS statistik menghasilkan nilai yang cukup baik. Pada analisa perbandingan waktu file hasil enkripsi terdapat siginifikansi perubahan waktu dengan parameter yang dihasilkan yaitu 3,5%, Pada analisa perbandingan ukuran file hasil enkripsi terdapat siginifikansi perubahan data dengan parameter yang dihasilkan yaitu dibawah 0,001%. Untuk serangan *Known-plainteks attack* pada algoritma *Secure Hill Cipher* berbasis kode ASCII memiliki tingkat kemanan yaitu 1,956% sedangkan berbasis *MonoAlphabetic* memiliki tingkat kemanan yaitu 0,536% dimana kedua basis tersebut tergolong aman. Hasil dari penelitian ini menunjukkan tingkatan perbandingan algoritma *Secure Hill Cipher* berasis kode ASCII dan *MonoAlphabetic* dari beberapa jenis serangan bahwa kedua basis tersebut tergolong bagus dan aman untuk digunakan untuk melakukan pengamanan data.

Kata Kunci: Kriptografi, *Secure Hill Cipher*, ASCII, *Monoalphabetic*

PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data,pesan dan informasi. Pengirim suatu pesan, data dan informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi.

Dengan perkembangan teknologi informasi sekarang ini yang begitu pesat, di mana setiap orang akan mudah untuk mendapatkan suatu pesan, data maupun informasi penting tersebut. Berbagai cara dilakukan orang untuk bisa mendapatkan data dan informasi penting tersebut. Mulai dari cara yang paling sederhana sampai dengan cara-cara yang lebih rumit. Dan berbagai cara pula orang berusaha untuk melindungi pesan tersebut agar tidak dapat diketahui oleh orang yang tidak memiliki hak atas pesan atau data tersebut.

Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang memiliki beberapa kelebihan dalam enkripsi data. Untuk menghindari matrik kunci yang tidak invertible, matrik kunci dibangkitkan menggunakan koefisien binomial newton. Proses enkripsi dan deskripsi menggunakan kunci yang sama, plaintext dapat menggunakan media gambar atau text. Algoritma Hill Cipher menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks..

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929 . Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Reddy, Vishnuvardhan, & Krishna, 2012)

Berdasarkan penelusuran terhadap penelitian yang relevan , Goyal et al. (2015) telah banyak melakukan studi dan penelitian terkait perbandingan Hill cipher hasil modifikasi matriks kunci dari berbagai sumber. Jenis Hill

cipher yang digunakan yaitu dengan menggunakan basis ASCII dan monoalphabetic sebagi generate matriks kunci. Analisis dilakukan dengan membandingkan total ukuran kunci yang dapat diterka pada brute force attack, menghitung total pasangan huruf yang dapat dicari, membandingkan kemunculan karakter terhadap frequency analysis attack dan melihat hasil output informasi plaintext yang sesuai yang dapat ditebak dari ciphertext terhadap serangan know-plaintext attack. Berdasarkan ketiga parameter tersebut, hasil analisis dilampirkan dalam bentuk tabel analisa perbandingan.

LANDASAN TEORI

A. **Kriptografi**

Kriptografi adalah suatu metode keamanan untuk melindungi suatu informasi dengan menggunakan kata-kata sandi yang hanya bisa dimengerti oleh orang yang berhak mengakses informasi tersebut. Kriptografi merupakan satu-satunya metode yang digunakan untuk melindungi informasi yang melalui jaringan komunikasi yang menggunakan *landline* (kabel di bawah tanah), satelit komunikasi, dan fasilitas microwave (gelombang mikro) (Hoffstein, Pipher, & Silverman, 2008).

Kriptografi adalah ilmu yang bersandarkan pada matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan autentikasi entitas (Sean-Philip Oriyano, Tanna, Sanghani, Ayushi, & Anderson, 2010).

Secara garis besar, kriptografi merupakan sebuah tehnik pengamanan suatu informasi yang dilakukan dengan mengolah informasi awal (plainteks) dengan perhitungan matematika, misalnya menggunakan algoritma enkripsi yang sudah ditemukan sehingga menghasilkan suatu informasi baru

(ciphertext) yang tidak bisa dibaca langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi.

B. Hill Cipher

Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang memiliki beberapa kelebihan dalam enkripsi data. Untuk menghindari matrik kunci yang tidak *invertible*, matrik kunci dibangkitkan menggunakan *koefisien binomial newton*. Proses enkripsi dan deskripsi menggunakan kunci yang sama, *plaintext* dapat menggunakan media gambar atau text. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks.

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929 . Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Reddy, Vishnuvardhan, & Krishna, 2012).

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext*. Teknik kriptanalisis ini disebut *known-plaintext attack*.

Algoritma proses enkripsi *Hill Cipher* adalah sebagai berikut.

1. Korespondenkan abjad dengan numerik A → 1, B → 2,…, Z → 26.
2. Buat matriks kunci berukuran m x m.

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

Matrik K merupakan matriks yang *invertible* yaitu memiliki *multiplicative inverse* K^{-1} sehingga $K.K^{-1} = 1$

3. *Plainteks* P = p1 p2 … pn , diblok dengan ukuran sama dengan baris atau kolom matrik K.

$$P_{mxq} = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1q} \\ p_{21} & p_{22} & \dots & p_{2q} \\ \dots & \dots & \dots & \dots \\ p_{m1} & p_{m2} & \dots & k_{mq} \end{bmatrix}$$

4. Kalikan Matrik K dengan Matrik P transpose dalam modulo 26.

$$C = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1q} \\ p_{21} & p_{22} & \dots & p_{2q} \\ \dots & \dots & \dots & \dots \\ p_{m1} & p_{m2} & \dots & k_{mq} \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1q} \\ c_{21} & c_{22} & \dots & c_{2q} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mq} \end{bmatrix}$$

5. Ubah hasil kedalam abjad menggunakan koresponden abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks.

Sebaliknya, Algoritma proses dekripsi *Hill Cipher* adalah sebagai berikut.

1. Korespondekan abjad dengan numerik.

2. Ubah *ciphertext* kedalam numerik.
3. Kunci yang digunakan untuk mendekrip *ciphertext* ke *plaintext* adalah invers dari matrik kunci K mxm.
4. Menghitung K −1.
5. Kalikan invers matriks kunci dengan *ciphertext* transpose dalam modulo 26, diperoleh plainteks transpose Pt = K −1Ct.
6. Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks.

Menurut (Ahmed, Sazzad, & Mollah, 2012) dalam kurun waktu yang sangat lama, *Hill cipher* dianggap tidak dapat dipecahkan sehingga dijadikan sistem pengiriman rahasia pada era Perang Dunia I dan masih digunakan secara luas. Seiring waktu, kriptanalisis terhadap *Hill Cipher* sangat sulit jika dilakukan dengan *ciphertext-only attack*, terlebih apabila matriks kunci yang digunakan berukuran besar. Kesulitan ini disebabkan oleh *ciphesrtext Hill Cipher* yang tidak memiliki pola dan setiap karakter dalam satu blok saling mempengaruhi karakter lainnya. Hal ini menjadi sebuah latar belakang beberapa peneliti dalam bidang kriptografi melakukan modifikasi algoritma kriptografi *hill cipher* antara lain dengan menggabungkan beberapa algoritma kriptografi klasik.

C. Algoritma *Secure Hill Cipher*

Untuk enkripsi algoritma *Secure Hill Cipher* mengambil huruf *plainteks* yang berurutan. *Secure Hill cipher*, masing-masing karakter diberi nilai numerik seperti a = 0, b = 1,…., z = 25. Subtitusi dari huruf *ciphertext* untuk m = 3, sistemnya akan di jelaskan sebagai berikut :

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) mod\ 26 \quad \text{.....(2.11)}$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) mod\ 26 \quad \text{.....(2.12)}$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) mod\ 26 \quad \text{.....(2.13)}$$

Kasus ini dapat dinyatakan dalam bentuk vektor kolom dan matriks :

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{23} & k_{33} \end{bmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \text{.....(2.14)}$$

Proses atau fungsi enkripsi (E) dapat dituliskan sebagai berikut.

$$E = C = E_k\,(P) = K_p \text{.....(2.15)}$$

Proses atau fungsi Dekripsi (D) dapat dituliskan sebagai berikut.

$$D = P = D_k\,(C) = k^{-1}C = k^{-1}K_p = P \text{.....(2.16)}$$

Sehingga dapat ditulis sebagai C = KP, dimana C dan P adalah vektor kolom dengan panjang 3, mewakili plaintext dan *ciphertext* masing-masing, dan K adalah matriks 3 × 3,yang merupakan kunci enkripsi. Semua operasi dilakukan mod 26. Jika panjang blok adalah m, ada 26 Kemungkinan blok huruf, masing-masing bisa dianggap sebagai huruf dalam alfabet 26 alfabet (Pommerening & Physik, 2014).

Modifikasi *Hill Cipher* terdapat pada Matriks dimana Setiap kunci pada matriks akan diputar satu elemen ke kanan relatif terhadapat vektor baris sebelumnya. Matriks sirkuler ini bisa kita sebut dengan A. algoritmnya secara umum adalah sebagai berikut:

1. Pilih matriks *n x n non-singular* G di GF (P) sebagai kunci publik sehingga det (Gc) = 0.

2. Pilih matriks $n\ x\ n$ utama A dalam GF (P) sebagai kunci rahasia.
3. Hitung Kunci $K = AGA^{-1} mod\ p$

Proses atau fungsi enkripsi *Secure Hill Cipher* adalah sebagai berikut.

1. M_i adalah blok *plaintext* ukuran n.
2. C_i adalah blok *cipher*.
3. $C_i = KM_i + V_i^T mod\ p$ dimana V_i adalah baris sirkuler matriks utama A.

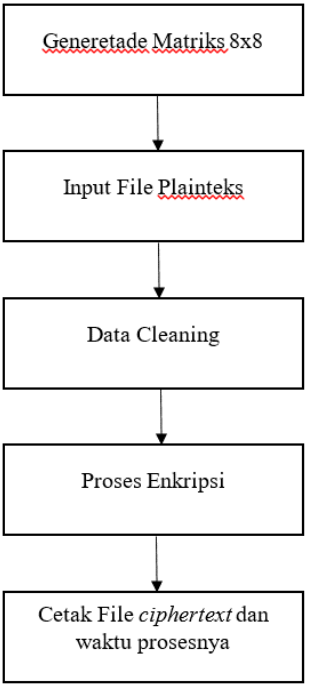
Proses atau fungsi dekripsi *Secure Hill Cipher* adalah sebagai berikut.

1. Hitung nilai $K^{-1} = AG^{-1}A^{-1}\ mod\ p$.
2. $M_i = K^{-1}(C_t - V_i^T)\ mod\ p$.

Disini V adalah baris pertama matriks A. Untuk setiap enkripsi blok *plaintext* yang kita gunakan berbeda dengan vector V berdasarkan rotasinya (Reddy et al., 2012).

METODOLOGI PENELITIAN

Perancangan dan pembuatan program merupakan salah satu langkah untuk mengimplementasikan algoritma secure hill cipher berbasis ASCII dan monoalphabetic pada proses enkripsi dan dekripsi. Bahasa pemograman yang digunakan adalah java SE (Standard Edition).untuk implemntasi algoritma enkripsi dan dekripsi Secure hill cipher salah satunya ditunjukkan pada gambar 1

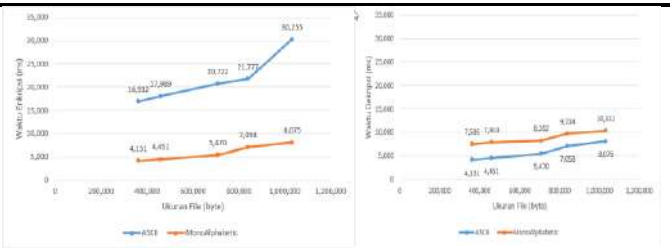


Gambar 1 implemntasi algoritma enkripsi Secure hill Cipher

HASIL DAN ANALISIS

A. Durasi Waktu

Gambar 3.1 merupakan Durasi waktu proses dari program enkripsi dan dekripsi yang telah dirancang dan diimplementasikan menjadi salah satu analisis. Dalam prosesnya, digunakan 3 kali perulangan untuk mendapatkan nilai dari durasi waktu proses enkripsi dan dekripsi yang optimal.



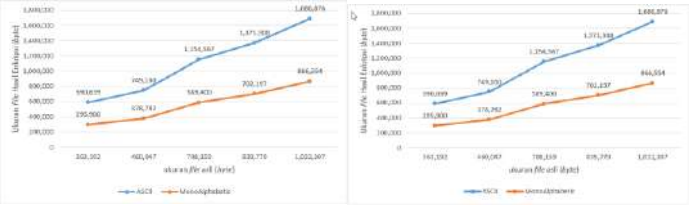
(a) (b)

Gambar 2 Perbandingan durasi waktu proses (a). Enkripsi, (b). Dekripsi .

Dari gambar 2.a menunjukkan perbandingan durasi waktu proses enkripsi dari Algoritma Secure Hill Cipher berbasis kode ASCII dan MonoAlphabetic, pada algoritma berbasis ASCII memiliki waktu yang lebih besar dibandingkan dengan basis MonoAlphabetic, Ini dikarenakan pada saat proses dekripsi Algoritma tersebut, pembentukan kunci memiliki tahapan yang lebih panjang dari pada tahapan pembentukan pada saat dilakukan enkripsi dan Dari gambar 2.b menunjukkan perbandingan durasi waktu proses dekripsi dari Algoritma Secure Hill Cipher berbasis kode ASCII dan MonoAlphabetic yang memiliki perbedaan durasi yang tidak signifikan. Hasil uji signifikan dapat dilihat pada lampiran 7 yang menunjukan nilai signifikan 0,35 di atas nilai tingkat signifikansi 0,05.

B. Ukuran File

Analisis ini dilakukan untuk membandingkan ukuran file hasil enkripsi dan dekripsi yang memiliki Input dan Output berupa sebuah file teks yang diterapkan pada setiap masing-masing data tersebut. Dengan menggunakan kunci yang sama pada saat proses Analisa menghitung durasi waktu proses enkripsi dan dekripsi, berikut ini merupakan data tabel perbandingan ukuran file hasil enkripsi algoritma Secure Hill Cipher yang ditunjukkan pada gambar 3.



(a) **(b)**

Gambar 3 Perbandingan Ukuran File (a). Enkripsi, (b). Dekripsi .

.

Dari gambar 3 Jika dibandingkan antara kedua algoritma Secure Hill Cipher ini, meski algoritma Secure Hill Cipher berbasis MonoAlphabetic memiliki efisien digunakan dari sisi penggunaan memori pada komputer, tetapi informasi yang terkandung pada algoritma tersebut sudah hilang. Sehingga membuat Secure Hill Cipher berbasis kode ASCII lebih diuntungkan dikarenakan informasi yang tetap terjaga dan tingkat kesulitan untuk mendapatkan informasi jugak lebih tinggi terhadap jenis serangan tertentu

4.1

4.2 C. Tabel Perbandingan Algoritma

Dari hasil analisis yang telah dilakukan pada penelitian ini, perbandingan algoritma Secure Hill Cipher berbasis kode ASCII dan MonoAlphabetic ditunjukkan pada tabel 1.

Tabel 1 Hasil Perbandingan Algoritma

No	Kategori	Algoritma *Secure Hill Cipher*	
		ASCII	***MonoAlphabetic***
1.	Jumlah Karakter	256	26
2.	Durasi waktu enkripsi	30,255 ms	15,179 ms
3.	Durasi waktu dekripsi	8,075 ms	10,332 ms

4.	Ukuran *File* hasil Enkripsi	61% lebih besar	17% lebih kecil
5.	Ukuran *File* hasil Dekripsi	0,99% lebih besar	17% lebih kecil
6.	Efisiensi Memori Komputer	tidak	iya
7.	Total Kombinasi Kunci	256^{64}	26^{64}
8.	Durasi waktu *Brute Force Attack*	$256^{64}\ x$ Satuan Waktu atau $1.63x10^{142}$ Hari	$26^{64}x$ Satuan Waktu atau $4.39x10^{78}$ Hari
9.	Korelasi analisis frekuensi	Tidak ada	Tidak ada
10.	Tingkat kemanan *Know-Plaintext attack*	aman	aman

Tabel 3.1. menunjukan bahawasanya tingkat kesulitan untuk melakukan jenis serangan tertentu pada algoritma Secure Hill Cipher berbasis kode ASCII sangat tinggi, diantaranya dapat dilihat dari jumlah karakter yang dapat digunakan adalah sebanyak 256, ini membuat nilai dari total kombinasi kunci jugak semakin besar lalu, durasi waktu untuk melakukan serangan Brute Force Attack menjadi sangat lama. Adapun yang menjadi isu lemahnya algoritma tersebut terhadap serangan Known-Plaintext attack sekarang sudah menjadi aman dikarenakan adanya sedikit modifikasi sederhana yang dilakukan pada saat pembentukan kunci pada algoritma tersebut.

KESIMPULAN

Algoritma Secure Hill Cipher berbasis kode ASCII dan MonoAlphabetic dari hasil analisa yang telah dilakukan pada penelitian ini sudah tidak lemah terhadap jenis serangan Know-Plaintext attack, dikarenakan adanya modifikasi sederhana tehadap pembentukan matrik kuncinya, ini yang membuat algoritma tersebut sudah sangat aman terhadap jenis serangan ini. Algoritma Secure Hill Cipher berbasis kode ASCII dan MonoAlphabetic dari

hasil analisa yang telah dilakukan pada penelitian ini sudah tidak lemah terhadap jenis serangan Know-Plaintext attack, dikarenakan adanya modifikasi sederhana tehadap pembentukan matrik kuncinya, ini yang membuat algoritma tersebut sudah sangat aman terhadap jenis serangan ini.

KEPUSTAKAAN

Abrams, M. D., & Podell, H. J. (2008). Cryptography. *International Journal of Computer Science Issues*, 350–385.

Agustina, E. R., Kurniati, A., Negara, L. S., Minggu, P., & Selatan, J. (2009). Pemanfaatan Kriptografi Dalam Mewujudkan. *Seminar Nasional Informatika 2009 (semnasIF 2009)*, *2009*(semnasIF), 22–28.

Ahmed, M., Sazzad, T. M. S., & Mollah, E. (2012). Cryptography and State-of-the-art Techniques. *International Journal of Computer Science Issues*, *9*(2), 583–586.

Andana, G. (2010). Analisis Frekuensi pada Teks Bahasa Indonesia Dan Modifikasi Algoritma Kriptografi Klasik, 1–9.

Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Cryptography*. *Springer* (Vol. XVI). https://doi.org/10.1007/978-0-387-77994-2.

Jain, J. (2017). Identify Cryptanalytic Brute-Force Attack Using Frequent Pattern Mining Blocking of Brute Force Attack, (May), 683–686.

Krishnan, K. (2004). Symmetric Key cryptosystem, 1–19.

Parmar, N. B., & Bhatt, D. R. (2007). Hill Cipher Modifications: A Detailed Review. *International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization)*, *3297*(3), 1467–1474. https://doi.org/10.15680/ijircce.2015.0303010

Pommerening, K., & Physik, F. (2014). Cryptology Part I : Classic Ciphers (Mathematical Version).

Reddy, K. A., Vishnuvardhan, B., & Krishna, A. V. N. (2012). A Modified Hill Cipher Based on Circulant Matrices. *Procedia Technology*, *4*, 114–118. https://doi.org/10.1016/j.protcy.2012.05.016.

Sean-Philip Oriyano, Tanna, J. M., Sanghani, M. P., Ayushi, M., & Anderson,

R. J. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, *1*(15), 73–114. https://doi.org/10.5120/331-502.

Shieny. (2008). Known Plaintext Attack History of the Known Plaintext Attack Breaking the Enigma Code How Good are Classic Ciphers ?.