

Nama : Rifko Satrio Rahmadani

Email : ikosatriorahmadani@gmail.com

Pekerjaan : Mahasiswa

Nama Instansi/Sekolah : Politeknik Negeri Bandung

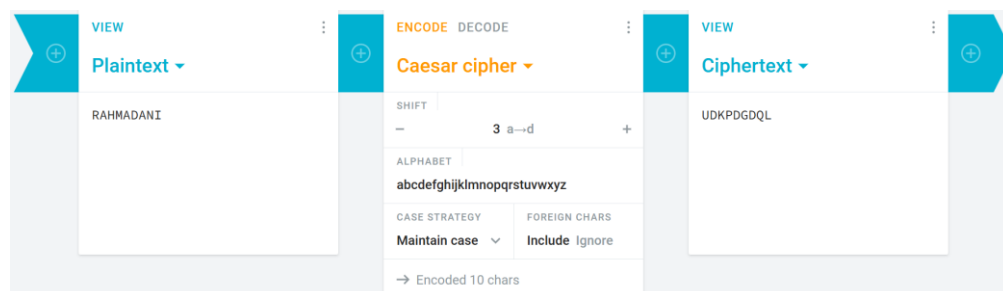
Challenge Dasar Cyptography

Challenge 1

- Plaintext: "RAHMADANI"
- Key = 3
- Proses Enkripsi:

No.	Plaintext	Pergeseran	Ciphertext
1	R	$R \rightarrow S (1) \rightarrow T (2) \rightarrow \mathbf{U (3)}$	U
2	A	$A \rightarrow B \rightarrow C \rightarrow \mathbf{D}$	D
3	H	$H \rightarrow I \rightarrow J \rightarrow \mathbf{K}$	K
4	M	$M \rightarrow N \rightarrow O \rightarrow \mathbf{P}$	P
5	A	$A \rightarrow B \rightarrow C \rightarrow \mathbf{D}$	D
6	D	$D \rightarrow E \rightarrow F \rightarrow \mathbf{G}$	G
7	A	$A \rightarrow B \rightarrow C \rightarrow \mathbf{D}$	D
8	N	$N \rightarrow O \rightarrow P \rightarrow \mathbf{Q}$	Q
9	I	$I \rightarrow J (1) \rightarrow K (2) \rightarrow \mathbf{L (3)}$	L

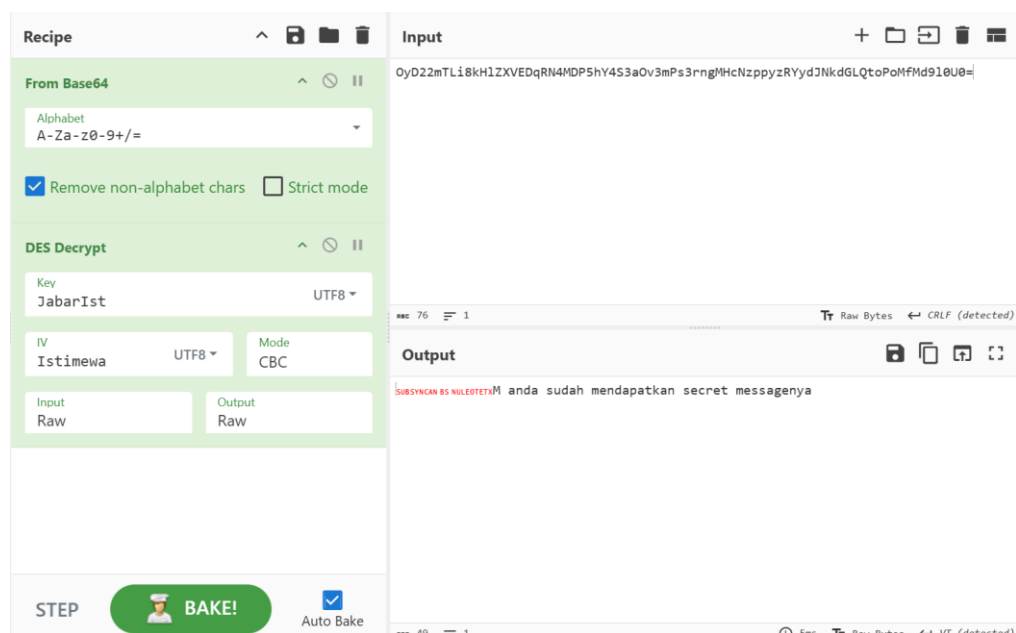
- Ciphertext: UDKPDGDQL
- Analisis: Caesar Cipher mengenkripsi teks dengan menggeser setiap huruf tiga langkah ke kanan. Dengan kunci +3, plaintext "RAHMADANI" berubah menjadi "UDKPDGDQL"
- Bukti Screenshoot:



Challenge 2

- Lakukan dekripsi untuk cipher berikut:
 - OyD22mTLi8kHIZXVEDqRN4MDP5hY4S3aOv3mPs3rngMHcNzppyzRY ydJNkdGLQtoPoMfMd9lOU0=
- Parameter Dekripsi:
 - Algoritma: DES
 - Mode: CBC
 - Key: JabarIst
 - IV: Istimewa
- Proses Dekripsi:

Ciphertext terlebih dahulu di-decode dari Base64, kemudian didekripsi menggunakan algoritma DES dengan mode CBC. Key dan IV diambil sesuai instruksi pada soal. Setelah proses dekripsi dijalankan di CyberChef, ciphertext berhasil dikembalikan menjadi plaintext.
- Plaintext: anda sudah mendapatkan secret messagenya
- Analisis: Setelah ciphertext di-decode dan didekripsi dengan key dan IV yang benar, hasilnya langsung muncul sebagai pesan asli.
- Bukti Screenshoot:



Challenge 3

- Buat dan Isi File dengan nama FBI.txt (Sebelum Diubah)
 - Ini merupakan data rahasia dari FBI, jaga keutuhan data ini!!!
- Hash SHA-256 (Sebelum Diubah)
 - SHA256:
AD29B0EB01656C9C68D0C771D1DA51926AE99532DC4D
F9297B6238294BA4CC38
- Edit isi File FBI.txt (Setelah Diubah)
 - Ini merupakan data RAHASIA dari FBI, jaga keutuhan data ini!!!
- Hash SHA-256 (Setelah Diubah)
 - SHA256:
E52F6DBB77B7389C5C6A5191DBBD76FE3087BDBD6DF3F
DF24ECF4401CA08A3C7
- Analisis: Dari hasil hashing, terlihat bahwa nilai SHA-256 pada file FBI.txt berubah total setelah isi filenya saya ubah sedikit. Ini menunjukkan bahwa fungsi hash sangat sensitif terhadap perubahan data. Perubahan menjadi kapital pun saja langsung menghasilkan hash baru yang benar-benar berbeda, sehingga bisa dipakai untuk memastikan apakah sebuah file masih utuh atau sudah dimodifikasi.
- Bukti Screenshoot:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ikosa> Get-FileHash "C:\Users\ikosa\OneDrive\Dokumen\Semester V\Cybersecurity\Pertemuan ke-6\FBI.txt" -Algo
rithm

Algorithm      Hash
-----
SHA256         AD29B0EB01656C9C68D0C771D1DA51926AE99532DC4D
F9297B6238294BA4CC38
C:\Users\ikosa\OneDrive\Dokum...

PS C:\Users\ikosa> Get-FileHash "C:\Users\ikosa\OneDrive\Dokumen\Semester V\Cybersecurity\Pertemuan ke-6\FBI.txt" -Algo
rithm

Algorithm      Hash
-----
SHA256         E52F6DBB77B7389C5C6A5191DBBD76FE3087BDBD6DF3F
DF24ECF4401CA08A3C7
C:\Users\ikosa\OneDrive\Dokum...

PS C:\Users\ikosa>
```

Challenge 4

- Ciphertext:
rfwn gjwxfrf rjrgfslzs ofgfw
- Proses Dekripsi:
 - Menggunakan metode Caesar Cipher sesuai clue.
 - Dilakukan brute force untuk mencoba seluruh pergeseran 1–25.
 - Mencari hasil plaintext yang paling masuk akal.
 - Ditemukan bahwa pergeseran 5 menghasilkan kalimat yang jelas dalam Bahasa Indonesia.
- Plaintext: mari bersama membangun jabar
- Analisis: Perubahan pergeseran pada setiap shift menunjukkan bahwa Caesar Cipher bekerja dengan cara mengganti setiap huruf berdasarkan jarak geser tertentu, dan hanya shift yang tepat yang dapat mengembalikan pesan asli
- Bukti Screenshoot:

The screenshot displays the dCode website's Caesar Cipher decoder. On the left, a search bar contains the ciphertext 'rfwn gjwxfrf rjrgfslzs ofgfw'. Below it, a list of results shows various shifts and their corresponding plaintexts. The result for a shift of 5 (key 21) is highlighted: 'mari bersama membangun jabar'. On the right, the 'CAESAR CIPHER DECODER' section shows the same ciphertext and a 'DECRYPT (BRUTEFORCE)' button. Below this, the 'MANUAL DECRYPTION AND PARAMETERS' section allows for manual decryption by selecting a shift or key. The 'CAESAR ENCODER' section is also visible, showing the same ciphertext and an 'ENCRYPT' button. The bottom of the page features a 'Support dCode' link.