

Nama : Rifko Satrio Rahmadani

Email : ikosatriorahmadani@gmail.com

Pekerjaan : Mahasiswa

Nama Instansi/Sekolah : Politeknik Negeri Bandung

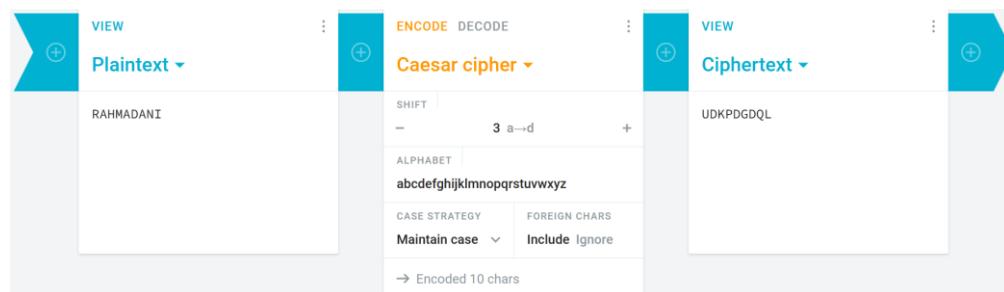
Challenge Dasar Cryptography

Challenge 1

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

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

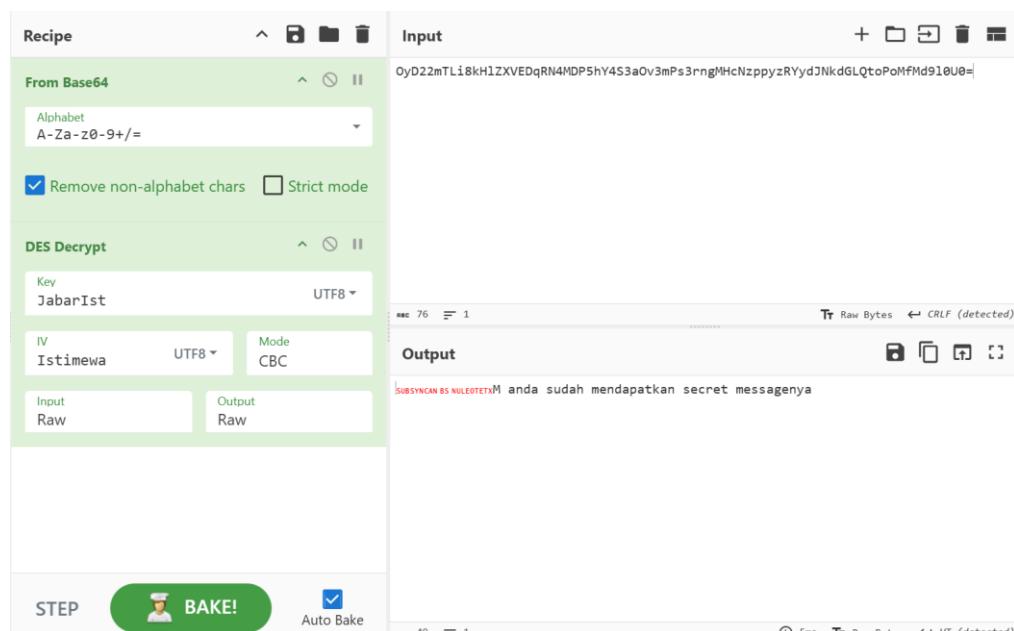
- Ciphertext: UDKPDGDQL
- Analisis: Caesar Cipher mengenkripsi teks dengan menggeser setiap huruf tiga langkah ke kanan. Dengan kunci +3, plaintext "RAHMADANI" berubah menjadi "UDKPDGDQL"
- Bukti Screenshoot:



Challenge 2

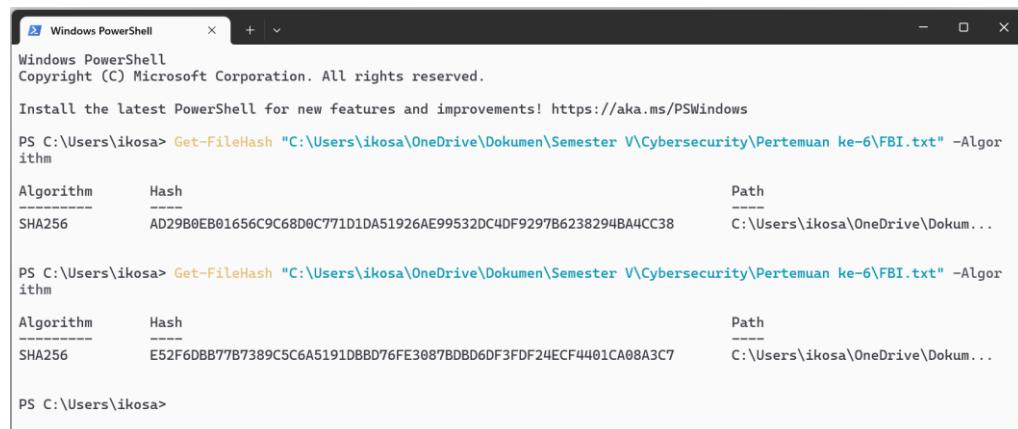
- Lakukan dekripsi untuk cipher berikut:
 - OyD22mTLi8kH1ZXVEDqRN4MDP5hY4S3aOv3mPs3rngMHC
NzppyzRY ydJNkdGLQtoPoMfMd9l0U0=
- Parameter Dekripsi:
 - Algoritma: DES
 - Mode: CBC
 - Key: JabarIst
 - IV: Istimewa
- Proses Dekripsi:

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 Screenshot:



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" -Algorithm SHA256
Algorithm      Hash                               Path
-----      -----
SHA256        AD29B0EB01656C9C68D0C771D1DA51926AE99532DC4D F9297B6238294BA4CC38
C:\Users\ikosa\OneDrive\Dokumen\Semester V\Cybersecurity\Pertemuan ke-6\FBI.txt

PS C:\Users\ikosa> Get-FileHash "C:\Users\ikosa\OneDrive\Dokumen\Semester V\Cybersecurity\Pertemuan ke-6\FBI.txt" -Algorithm SHA256
Algorithm      Hash                               Path
-----      -----
SHA256        E52F6DBB77B7389C5C6A5191DBBD76FE3087BDBD6DF3DF24ECF4401CA08A3C7
C:\Users\ikosa\OneDrive\Dokumen\Semester V\Cybersecurity\Pertemuan ke-6\FBI.txt

PS C:\Users\ikosa>
```

Challenge 4

- Ciphertext:
rfwn gjwxfrf rjrgfslz s 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 shows the dCode Caesar Cipher tool. At the top, there's a search bar with placeholder text "Search for a tool" and a dropdown menu showing "e.g. type 'caesar'". Below the search bar, there are two buttons: "BROWSE THE FULL DCODE TOOLS LIST" and "Results". The main area displays a list of results for the ciphertext "rfwn gjwxfrf rjrgfslz s ofgfw". Each result is a numbered string followed by its decryption key and a brief description. For example, the first result is "11 mari bersama membangun jabar". There are also sections for "CAESAR CIPHER DECODER" and "CAESAR ENCODER", both with dropdown menus for shift values (0-25) and various alphabet options. On the right side, there's a "Summary" sidebar with links to other cipher-related tools and a "Similar pages" sidebar with links to ROT Cipher, Shift Cipher, Vigenere Cipher, etc.