

Kelompok :

1. Andrey Hartawan Suwardi
2. Ivone Liwang
3. Franklin Jaya
4. Michael Sawitto

sistem kerja dari kelas `Shiapcrypto` berdasarkan kode Python, dengan fokus pada proses enkripsi dan dekripsi menggunakan kunci rahasia`AFVM`. Kode Rahasia bisa diganti menggunakan function updatekey().

Tabel ASCII Alphabet :

ASCII	Char	Hex	Bin		ASCII	Char	Hex	Bin
65	A	41	0100 0001		97	a	61	0110 0001
66	B	42	0100 0010		98	b	62	0110 0010
67	C	43	0100 0011		99	c	63	0110 0011
68	D	44	0100 0100		100	d	64	0110 0100
69	E	45	0100 0101		101	e	65	0110 0101
70	F	46	0100 0110		102	f	66	0110 0110
71	G	47	0100 0111		103	g	67	0110 0111
72	H	48	0100 1000		104	h	68	0110 1000
73	I	49	0100 1001		105	i	69	0110 1001
74	J	4A	0100 1010		106	j	6A	0110 1010
75	K	4B	0100 1011		107	k	6B	0110 1011
76	L	4C	0100 1100		108	l	6C	0110 1100
77	M	4D	0100 1101		109	m	6D	0110 1101
78	N	4E	0100 1110		110	n	6E	0110 1110
79	O	4F	0100 1111		111	o	6F	0110 1111
80	P	50	0101 0000		112	p	70	0111 0000
81	Q	51	0101 0001		113	q	71	0111 0001
82	R	52	0101 0010		114	r	72	0111 0010
83	S	53	0101 0011		115	s	73	0111 0011
84	T	54	0101 0100		116	t	74	0111 0100
85	U	55	0101 0101		117	u	75	0111 0101
86	V	56	0101 0110		118	v	76	0111 0110
87	W	57	0101 0111		119	w	77	0111 0111
88	X	58	0101 1000		120	x	78	0111 1000
89	Y	59	0101 1001		121	y	79	0111 1001
90	Z	5A	0101 1010		122	z	7A	0111 1010

Sistem Kerja Kelas `Shiapcrypto`

1. Inisialisasi Kunci Rahasia

Ketika kelas Shiapcrypto diinisialisasi dengan kunci rahasia 'AFVM', metode `generate_keys` akan mengubah setiap karakter kunci menjadi nilai ASCII, lalu diubah menjadi biner:

- 'A' → 65 → 01000001
- 'F' → 70 → 01000110
- 'V' → 86 → 01010110
- 'M' → 77 → 01001101

Nilai biner ini disimpan dalam variabel:

- B1 = 01000001
- B2 = 01000110
- B3 = 01010110
- B4 = 01001101

2. Proses Enkripsi

Misalkan teks yang ingin dienkripsi adalah 'HELLO'.

Langkah-langkah Enkripsi:

Untuk setiap karakter dari plaintext, akan dilakukan proses XOR bertahap.

Contoh untuk Karakter 'H':

- Nilai ASCII dari 'H' adalah 72, yang dalam biner adalah:
 1. `ord('H') = 72 → 01001000`
- Proses XOR dilakukan secara bertahap:
 2. `01001000 (H) ^ 01000001 (B1) → 00001001`
 3. `00001001 ^ 01000110 (B2) → 01001111`
 4. `01001111 ^ 01010110 (B3) → 00011001`
 5. `00011001 ^ 01001101 (B4) → 01010100`
- Hasil akhir dalam biner: 01010100, yang merupakan karakter 'T'.

Untuk Karakter 'E':

- Nilai ASCII 'E' adalah 69 → 01000101
- Proses XOR :
 1. `01000101 ^ 01000001 (B1) → 00000100`
 2. `00000100 ^ 01000110 (B2) → 01000010`
 3. `01000010 ^ 01010110 (B3) → 00010100`

4. $00010100 \wedge 01001101$ (B4) $\rightarrow 01011001$
- Hasil akhir: $01011001 \rightarrow 'Y'$.

Karakter 'L' (pertama):

- Nilai ASCII 'L' adalah 76 $\rightarrow 01001100$
- Proses XOR :
 1. $01001100 \wedge 01000001$ (B1) $\rightarrow 00001101$
 2. $00001101 \wedge 01000110$ (B2) $\rightarrow 01001011$
 3. $01001011 \wedge 01010110$ (B3) $\rightarrow 00011101$
 4. $00011101 \wedge 01001101$ (B4) $\rightarrow 01010000$
- Hasil akhir: $01010000 \rightarrow 'P'$.

Karakter 'O':

- Nilai ASCII 'O' adalah 79 $\rightarrow 01001111$
- Proses XOR :
 1. $01001111 \wedge 01000001$ (B1) $\rightarrow 00001110$
 2. $00001110 \wedge 01000110$ (B2) $\rightarrow 01000100$
 3. $01000100 \wedge 01010110$ (B3) $\rightarrow 00011110$
 4. $00011110 \wedge 01001101$ (B4) $\rightarrow 01010011$
- Hasil akhir: $01010011 \rightarrow 'S'$.

Jadi, teks terenkripsi dari 'HELLO' adalah 'TYPPS'.

3. Proses Dekripsi

Proses dekripsi menggunakan algoritma yang sama, tetapi dengan proses yang dilakukan secara terbalik dari proses enkripsi.

Langkah-langkah Dekripsi:

Karakter 'T':

- Nilai ASCII 'T' adalah 84 $\rightarrow 01010100$
- Proses XOR bertahap :
 1. $01010100 \wedge 01001101$ (B4) $\rightarrow 00011001$
 2. $00011001 \wedge 01010110$ (B3) $\rightarrow 01001111$
 3. $01001111 \wedge 01000110$ (B2) $\rightarrow 00001001$
 4. $00001001 \wedge 01000001$ (B1) $\rightarrow 01001000$
- Hasil akhir: $01001000 \rightarrow 'H'$.

Karakter 'Y':

- Nilai ASCII 'Y' adalah 89 $\rightarrow 01011001$
- Proses XOR bertahap :

1. $01011001 \wedge 01001101 \text{ (B4)} \rightarrow 00010100$
 2. $00010100 \wedge 01010110 \text{ (B3)} \rightarrow 01000010$
 3. $01000010 \wedge 01000110 \text{ (B2)} \rightarrow 00000100$
 4. $00000100 \wedge 01000001 \text{ (B1)} \rightarrow 01000101$
- Hasil akhir: $01000101 \rightarrow \text{'E'}$.

Karakter 'P' (pertama):

- Nilai ASCII 'P' adalah 80 $\rightarrow 01010000$
- Proses XOR bertahap :
 1. $01010000 \wedge 01001101 \text{ (B4)} \rightarrow 00011101$
 2. $00011101 \wedge 01010110 \text{ (B3)} \rightarrow 01001011$
 3. $01001011 \wedge 01000110 \text{ (B2)} \rightarrow 00001101$
 4. $00001101 \wedge 01000001 \text{ (B1)} \rightarrow 01001100$
- Hasil akhir: $01001100 \rightarrow \text{'L'}$.

Karakter 'S':

- Nilai ASCII 'S' adalah 83 $\rightarrow 01010011$
- Proses XOR bertahap :
 1. $01010011 \wedge 01001101 \text{ (B4)} \rightarrow 00011110$
 2. $00011110 \wedge 01010110 \text{ (B3)} \rightarrow 01000100$
 3. $01000100 \wedge 01000110 \text{ (B2)} \rightarrow 00001110$
 4. $00001110 \wedge 01000001 \text{ (B1)} \rightarrow 01001111$
- Hasil akhir: $01001111 \rightarrow \text{'O'}$.

Jadi, teks terenkripsi 'TYPPS' berhasil didekripsi kembali menjadi 'HELLO'.

Kesimpulan Sistem Kerja :

- Proses enkripsi dan dekripsi menggunakan operasi XOR pada nilai ASCII dari karakter.
- Setiap karakter diubah menjadi nilai ASCII menggunakan ``ord()``, di-XOR secara bertahap dengan empat kunci (``B1``, ``B2``, ``B3``, ``B4``), lalu diubah kembali menjadi karakter menggunakan ``chr()``.
- Algoritma yang sama digunakan untuk enkripsi dan dekripsi. (Kata kunci : XOR Binary untuk mendapatkan hasil yang di XOR)

Link Collab : [Projectes.ipynb](https://colab.research.google.com/drive/1_aFdZDpo-3DeK1nXRMqakrEddN3pZDk?usp=sharing)

https://colab.research.google.com/drive/1_aFdZDpo-3DeK1nXRMqakrEddN3pZDk?usp=sharing