CAPTURE THE FLAG WRITE UP

Dibuat oleh :
PORT80
(Johan Wahyudi)

COMNETS CTF SEASON 2
2015

CHALLENGE : CRYPTO
CASE : CRYPTO01 - "CIPHER POOL 9"
FLAG :COMNETS{Moehammad_Yamin}

1. Executive Summary

Penyandian Baconian
Penyandian Polybius Square
Penyandian AutoKey

2. Technical Report

Step 1 (penyandian baconian):

Encrypt text

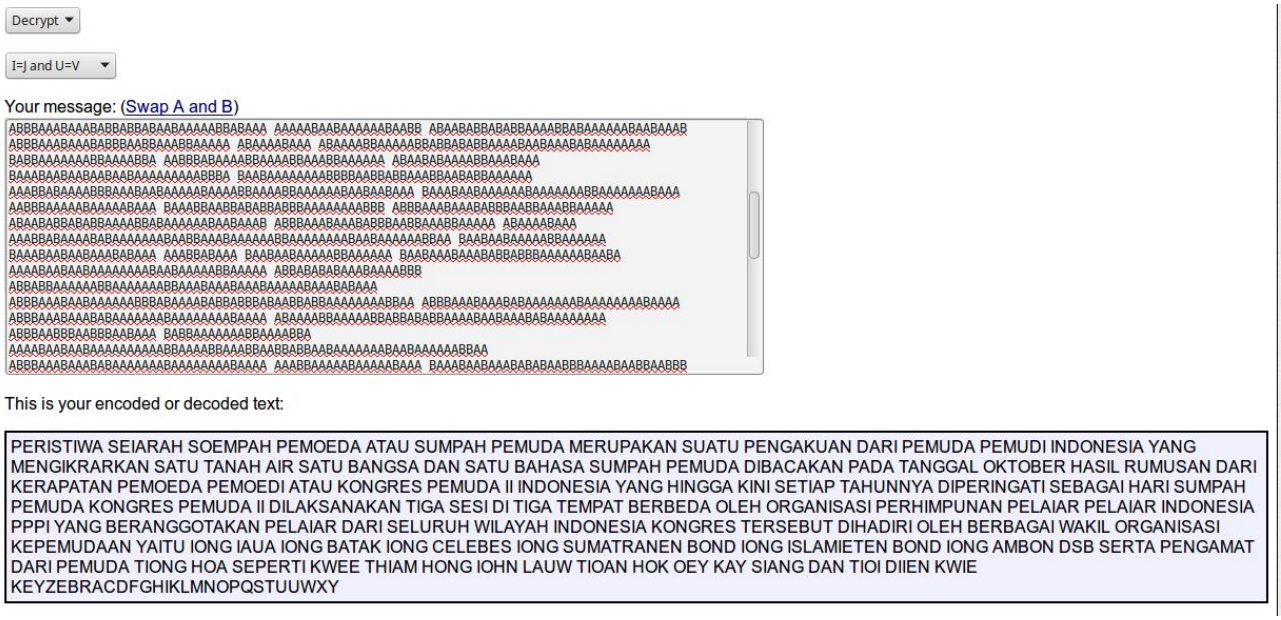
```
ABBBAAABAABAAAAABAAABAAABBAABAABAAABABAAAAAAA BAAABAABAAABAAAAAAAABAAAAAAAAAAABBB BAAABABBABAABAAABABBABBBAAAAAAAAABBB
ABBBAAABAAABABBABBABAABAAAAABBAAAAA AAAAABAABAAAAAAABAABB BAAABBAABBABABBABBBAAAAAAAAABBB ABBBAAABAAABABBBAABBAAABBAAAAA
ABABBAABAABAAAABAABBABBBAAAAAAABAABAAAAAABBAA BAAABBAABBAAAAABAABABAABB ABBBAAABAAABBAAAABBAAAAAAABAABBAABBAAAAAABBAA
AAABBAAAAABAAAAABAAA ABBBAAABAAABABBBAABBAAABBAAAAA ABBBAAABAAABABBBAABBAAABBABAAA ABAAAABBAAAAABBABBABABBAAAABAABAAABABAAAAAAAA
BABBAAAAAAAABBAAAABBA ABABBAABAAABBAAAABBAABAAAABAABBAAAAAAAAAABAAAAABAABAAAAAABBAA BAAABAAAAABAABABAABB BAABAAAAAAABBAAAAAAAAABBB
AAAAAABAAABAAAA BAAABAAAAABAABABAABB AAAABAAAAAABBAAAABBABAAABAAAAA AAABBAAAAAABBAA BAAABAAAAABAABABAABB AAAABAAAAAAABBBAAAAABAAABAAAAA
BAAABBAABBABABBABBBAAAAAAAAABBB ABBBAAABAAABABBBAABBAAABBAAAAA AAABBABAAAAAAABAAAAAAAABAAAAAAABAABAAAAAABBAA ABBBAAAAAAAAAABBAAAAA
BAABAAAAAAAABBAAAABBAAABBAAAAAAAABABA ABBABABAABBAABAABBABAAAABAABAABAAAA AABBBAAAAABAAABABAAAABABA BAAAABAABBABABBBAABBBAAABAAAAAABBAA
AAABBAAAAABAAAAABAAA ABAABAABAABAAAAAAAAAABBBAAAAAABAABAAAAAAABBAA ABBBAAABAAABABBABBABAABAAAAABBAAAAA
ABBBAAABAAABABBABBABAABAAAAABBABAAA AAAAABAABAAAAAAABAABB ABAABABBABABBAAAABBABAAAAAABAABAAAB ABBBAAABAAABABBBAABBAAABBAAAAA ABAAAABAAA
ABAAAABBAAAAABBABBABABBAAAABAABAAABABAAAAAAAA BABBAAAAAAAABBAAAABBA AABBBABAAAABBAAAABBAAABBAAAAAA ABAABABAAAABBAAABAAA
BAAABAABAABAABAABAAAAAAAAAABBBA BAABAAAAAAAAABBBBAABBABBAAABBAABABBAAAAAA AAABBABAAAABBBAAABAABAAAAABAAAABBAAAABBAAAAAABAABAABAAA
BAAABAABAAAAAABAAAAAAABBAAAAAAAABAAA AABBBAAAAABAAAAABAAA BAAABBAABBABABBABBBAAAAAAAAABBB ABBBAAABAAABABBBAABBAAABBAAAAA
ABAABABBABABBAAAABBABAAAAAABAABAAAB ABBBAAABAAABABBBAABBAAABBAAAAA ABAAAABAAA
AAABBABAAAABABAAAAAAAABAABBAAABAAAAAABBAAAAAAAAABAABAAAAAAABBAA BAABAABAAAAABBAAAAAA BAAABAABAABAAABABAAA AAABBABAAA BAABAABAAAAABBAAAAAA
BAABAAABAAABABBABBBAAAAAABAABA AAAABAABAABAAAAAAAAABAABAAAAABBAAAAA ABBABABABAAABAAAABBB
ABBABBAAAAAABBAAAAAAABBAAABAAABAAABAAAAABAAABABAAA ABBBAAABAABAAAAAABBBABAAAABABBABBBABAABBABBAAAAAAAABBAA
ABBBAAABAAABABAAAAAAAABAAAAAAAAABAAAA ABBBAAABAAABABAAAAAAAABAAAAAAAAABAAAA ABAAAABBAAAAABBABBABABBAAAABAABAAABABAAAAAAAA
ABBBAABBBAABBBAABAAA BABBAAAAAAAABBAAAABBA AAAABAABAABAAAAAAAAAABBAAAABBAAABBAABBABBAABAAAAAAAABAABAAAAAAABBAA
ABBBAAABAAABABAAAAAAAABAAAAAAAAABAAAA AAABBAAAAABAAAAABAAA BAAABAABAAABABABAABBBAAAABAABBAABBB BABAAABAAAABABAAAAAABABBAAAAAAAAABBB
ABAAAABBAAAAABBABBABABBAAAABAABAAABABAAAAAAAA ABAABABBABABBAAAABBABAAAAAABAABAAAB BAABAAABAABAAAABAAABAABAAAAAABBAABBBAABA
AAABBABAAAAABBBAAAAAAAABBABAAABAAAAABAAA ABBABABABAAABAAAABBB AAAABAABAABAAAAAAAABAAAAAAABBAAAAAAAABAAA BABAAAAAAAABAABABAAAABABA
ABBABBAAAAAABBAAAAAAABBAAABAAABAAABAAAAABAAABABAAA ABAABAABAAABBBAAABAAABABBBAABBAAABBAAAAAAAAAAAABBAA BABBAAAAAAAABAAABAABABAABB
ABAAAABBABABBAAAABBA ABAAAAAAAABAABBAAAAA ABAAAABBABABBAAAABBA AAAABAAAAABAABAAAAAAAABAAB ABAAAABBABABBAAAABBA
AAABAAABAAABABAAABAAAAAABAABAABAAAB ABAAAABBABABBAAAABBA BAAABBAABBABABBAAAAABAABABAAAAAAAAAAABBAAAABAAABBAA AAAABABBABABBAAAAABB
ABAAAABBABABBAAAABBA ABAAABAAABABABAAAAAAABABBBABAAAAABAABAABAAABAAABBAA AAAABABBABABBAAAAABB ABAAAABBABABBAAAABBA
AAAAAABABBAAAABABBABABBAA AAABBBAAABAAAAB BAAABAABAABAAAABAABAAAAAA ABBBAAABAAABBAAAABBAAAAAAABABBAAAAABAABA AAABBAAAAABAAAAABAAA
ABBBAAABAAABABBBAABBAAABBAAAAA BAABAABAAAABBABABBAAAABBA AABBBABBABAAAAA BAAABAABAAABBBAAABAABAAAABAABAABAAA ABAABBABAAAABAAAABAA
BAABAAABBBABAAAAAAAAAABABB AABBBABBABABBAAAABBA ABAAAABBABAABBBABBAA ABABAAAAAAABAABBBABAA BAABAABAAAABBABAAAAAABBAA AABBBABBABABAAB
ABBABAABAABABBA ABAABAAAAABABBA BAAABABAAAAAAAAAABBAAAABBA AAABBAAAAAABBAA BAABAABAAAABBABABAAA AAABBABAAAABAAAAABAAABBAA
ABAABBABAAABAAAAABAA
ABAABAABAABABBABABBBAABAAAAAABBAAAAAAAAAAAABAAAABBAABABAABBAAABBBABAAAABAABABABAABABBABBAAABBABABBBAABBBBAAABBAABABAABBBAABBBABAABABABB
ABBA
```

Sandi Bacon (The Baconian Cipher) adalah salah satu sandi yang memakai metode steganography (metode menyembunyikan pesan dalam sebuah pesan rahasia) yang diciptakan oleh Francis Bacon pada tahun 1605.

Untuk memecahkan pesan, setiap kata dalam pesan yang sudah dalam bentuk sandi Bacon tersebut harus dibagi per 5 kelompok dalam bentuk 'a' atau 'b'. Untuk teks sandi utamanya, berikut ini list nya :

A = aaaaa	I/J = abaaa	R = baaaa
B = aaaab	K = abaab	S = baaab
C = aaaba	L = ababa	T = baaba
D = aaabb	M = ababb	U/V = baabb
E = aabaa	N = abbaa	W = babaa
F = aabab	O = abbab	X = babab
G = aabba	P = abbba	Y = babba
H = aabbb	Q = abbbb	Z = babbb

Disini saya menggunakan tools online (http://rumkin.com/tools/cipher/baconian.php) untuk men-decrypt pesan di atas



Setelah di decrypt, di akhir pesan terdapat key “ZEBRACDFGHIKLMNOPQSTUUWXY”, dan sepertinya proses pemecahan sandi belum selesai, kita lanjut ke step selanjutnya

Step 2 (Penyandian Polybius Square) :

Encrypt Text :
ADAEDBAEDEDBABADDEAECDAEDDAEACDEEABDABBBEACEBDBBAECCAECDDDAECDACEAD
EAECECEEEAECBABDEEAAEDBDBDBCADDEABDDACEBBDABBCADACADADBEADDDBCADEDA
ACABADBEAEADAEDBCBDACEBDADABDDCACECABBAEDBAEDECDABCDDBABADCBEAAEDE
DDABCDAECEBDAEDEDBABADDDAEDEEAAECEBBAECCAECDDDAECEEAACAEADCADBAEADA
EDBABCDEABBAEAEBAAEADAEBBCACCAECECAEADECBAECEBBABCEBDAECEEAADAECAAEC
ECDDAABBEAECDCDAEBBEEAECDCACEDEABCEDEAECEBDAEADDECABBAECEBEEAACEACEB
DAECEDBABADDDAEDEEAAECEBBABCEBDAECEDBABCDEABBAECDABCEEAADEADECEEEAEA
EBBAECCCACDAEBCAECBDEDAADEEAECEBDACCADDAECDABCDDBABADCBEAAEDEDBABAD
DDAEDEEAAECECACEBBDACEABDDCAAEEEAECADEEADDABCAAEADAEBEACAEBEAEDDAEB
EEACBEACDAEBBAEDEDBABCEBBCABBCACBAECEBBAECECBABCDAEEAAECECBABEEBADAC
DCEABDEDDBADEBC
Key : ZEBRACDFGHIKLMNOPQSTUUWXY

Polybius square cipher secara umum merupakan teknik enkripsi yang berfungsi untuk mengubah suatu pesan menjadi angka tertentu dengan menggunakan tabel yang telah ditetapkan. Pesan ini akan menjadi suatu angka yang berpasangan menurut petunjuk dari tabel dan setiap angka yang berpasangan mewakili suatu karakter/huruf/angka.
Contoh tabel penyandian Polybius squere ukuran 5x5 :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Untuk mendecrypt pesan di atas saya menggunakan pycipher (modul python), dengan key ZEBRACDFGHIKLMNOPQSTUUWXY, ukuran 5x5, dan Ciphertext characters ABCDE,karena karakter yang ada di ciphertext hanya huruf ABCDE,

```
johan sandi # python
Python 2.7.6 (default, Jun 22 2015, 17:58:13)
[GCC 4.8.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from pychiper import PolybiusSquere
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
ImportError: No module named pychiper
>>> from pycipher import PolybiusSquere
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
ImportError: cannot import name PolybiusSquere
>>> from pycipher import PolybiusSquare
>>> p = PolybiusSquare ('ZEBRACDFGHIKLMNOPQSTUUWXY' ,5,'ABCDE')
>>> p.decipher('ADAEDBAEDEDBABADDEAECDAEDDAEACDEEABDABBBEACEBDBBAECCAECDDDAECDACEADEAECECEEEAECBABDEEAAEDBDBDBCADDEABDDACEBBDAB
BCADACADADBEADDDBCADEDAACABADBEAEADAEDBCBDACEBDADABDDCACECABBAEDBAEDECDABCDDBABADCBEAAEDEDDABCDAECEBDAEDEDBABADDDAEDEEAAECEBBAE
CCAECDDDAECEEAACAEADCADBAEADAEDBABCDEABBAEAEBAAEADAEBBCACCAECECAEADECBAECEBBABCEBDAECEEAADAECAAECECDDAABBEAECDCDAEBBEEAECDCACED
EABCEDEAECEBDAEADDECABBAECEBEEAACEACEBDAECEDBABADDDAEDEEAAECEBBABCEBDAECEDBABCDEABBAECDABCEEAADEADECEEEAEAEBBAECCCACDAEBCAECBDE
DAADEEAECEBDACCADDAECDABCDDBABADCBEAAEDEDBABADDDAEDEEAAECECACEBBDACEABDDCAAEEEAECADEEADDABCAAEADAEBEACAEBEAEDDAEBEEACBEACDAEBBA
EDEDBABCEBBCABBCACBAECEBBAECECBABCDAEEAAECECBABEEBADACDCEABDEDDBADEBC')
'RAPATPERTAMASABTUGEDUNGDALAMSAMBUTANNYAKETUAPPPISUGONDODIOIOPUSPITOBERHARAPKONGRESINIDAPATMEMPERKUATSEMANGATPERSATUANDALAMSANU
BARIPARAPEMUDAACARADILANIUTKANDENGANURAIANMOEHAMMADYAMINTENTANGARTIDANHUBUNGANPERSATUANDENGANPEMUDAMENURUTNYAADALIMAFAKTORYANGB
ISAMEMPERKUATPERSATUANINDONESIAYAITUSEIARAHBAHASAHUKUMADATPENDIDIKANDANKEMAUANKEYCOMNETSCTF'
>>>
```

Setelah di decrypt,di akhir pesan ada tulisan key,yaitu COMNETSCTF, itu berarti tugas kita belum selesai, lanjut lagi,

Step 3 (Penyandian Autokey):

Ciphertext :
Uwmcedsjmtcwhnaxgtxalsygkntmvfjtvzcagurgltrxsniymhge
Key ; COMNETSCTF

Kriptografi Autokey adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kriptografi caesar dan vegenere. Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi. Rumus yang berlaku untuk kriptografi Autokey sama dengan untuk Caesar dan Vigenere.

$C=E(P)=(P+k)$
mod26
$P=D(C)=(C-k)$
mod26

Contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA. Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere, aturan penyandian caesar dan vigenere cari sendiri ya... :))

Table penyandian Autokey :

```
    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
    ---------------------------------------------------
A   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
B   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 A
C   C 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
D   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
E   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 D
F   F 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
G   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
H   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 G
I   I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J   J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K   K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L   L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M   M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N   N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O   O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P   P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q   Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R   R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S   S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T   T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U   U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V   V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W   W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X   X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y   Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z   Z 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
```

Sama seperti step 2, saya menggunakan modul pycipher untuk mendecrypt pesan ini,

```
johan sandi # python
Python 2.7.6 (default, Jun 22 2015, 17:58:13)
[GCC 4.8.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from pycipher import Autokey
>>> Autokey ('COMNETSCTF').decipher('uwmcedsjmtcwhnaxgtxalsygkntmvfjtvzc
agurgltrxsniymhge')
'SIAPAKAHTOKOHYANGMEMBERIKANARTIPERSATUANDENGANPEMUDA'
>>> LOL :p haha..
```

Setelah di decrypt, hasilnya adalah SIAPAKAH TOKOH YANG MEMBERIKAN ARTI PERSATUAN DENGAN PEMUDA,
karena saya cinta dengan indonesia dan pelajaran sejarah waktu SD dulu saya dapat nilai 9, :v jadi saya masih ingat kalo yang memberikan arti tersebut sekaligus yang merumuskan ikrar sumpah pemuda adalah bapak Moehammad yamin, yupp.. Ternyata benar flagnya adalah COMNETS{Moehammad_Yamin}

3. *Conclusion*

Flag : COMNETS{Moehammad_Yamin}

4. *Reference*

http://practicalcryptography.com

CHALLENGE : CRYPTO
CASE : CRYPTO04 - "Klaue"
FLAG : COMNETS{TANAHAIRKUINDONESIA}

1. *Executive Summary*

Image Fussion (Penggabungan Citra)
Tools : GIMP

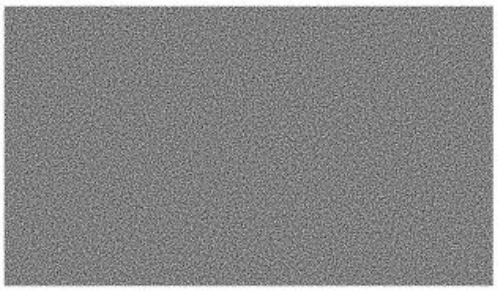
2. *Technical Report*

Image Fussion adalah salah satu teknik pemrosesan citra digital, image fusion dapat mengakomodasi kebutuhan citra resolusi tinggi tanpa harus mengusahakan sistem pencitraan dengan *resolving power* yang tinggi,

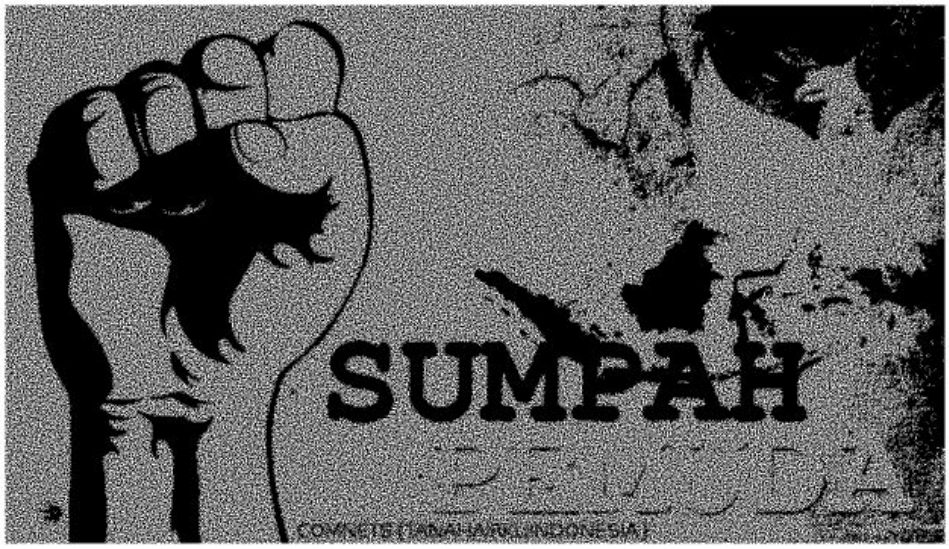
Citra multispektral (a), Citra Pankromatik (b) dan Citra gabungan (c)

(Contoh Penggabungan Image)

pada kasus kali ini kita mendapat 2 file photo, (photo di bawah setelah disandingkan)



Tidak ada informasi sama sekali di photo diatas, namun setelah photo tersebut di gabung menjadi satu,barulah info di dapat,



Setelah di zoom, Yupp... flagnya mulai kelihatan,

3. *Conclusion*

Flag : COMNETS{TANAHAIRKUINDONESIA}

4. *Reference*

http://kihari.blogspot.co.id/2014/02/fusi-citra-image-fusion-dalam.html

CHALLENGE : CRYPTO
CASE : CRYPTO05 - "Porta"
FLAG : COMNETS{indonesiaraya}

5. *Executive Summary*

Encode : UUencode *Penyandian : ROT13* *Porta*

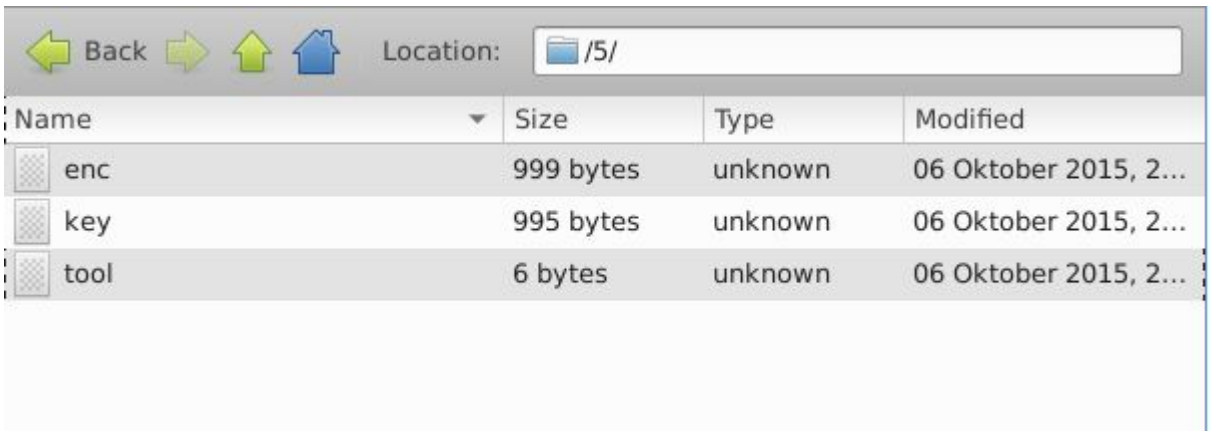
6. *Technical Report*

Step 1:
di berikan sebuah file compress tar.gz yg di dalamnya berisikan file 5.exe (file executable), tapi setelah di cek tipe filenya, ternyata isi filenya adalah text yang telah di encode dengan uuencoded atau xxencoded (setelah di cek lagi yg benar adalah UUencoded)

```
joe@joe:/media/joe/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/KRYPTO/crypto05 (2)$ file 5.exe
5.exe: uuencoded or xxencoded, ASCII text
joe@joe:/media/joe/MY-LIB/HACKING/CTF/CTF ILKOM/CTF SESASON 2/KRYPTO/crypto05 (2)$
```

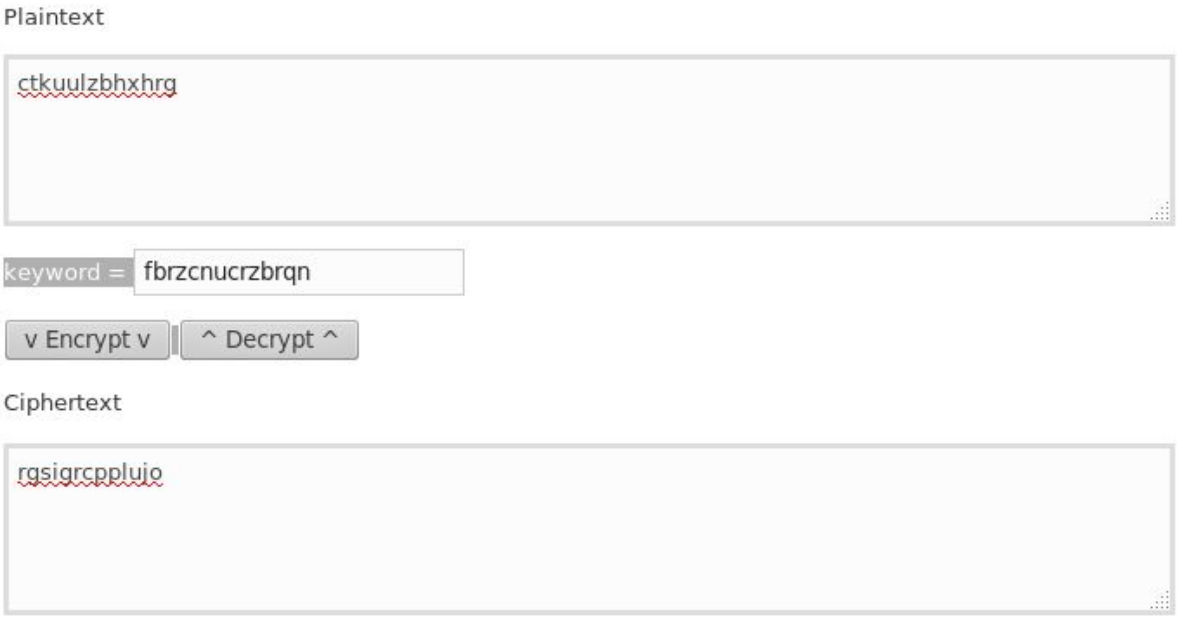
Saya disini menggunakan tools online di http://www.webutils.pl/index.php?idx=uu untuk mendecode,

Setelah di decode, Didapat file compress dengan nama 5.zip, yang isinya adalah :



Isi file enc : rgsigrcpplujo
Isi file key : fbrzcnucrzbrqn
Isi file tool : porta
Karena isi file tool adalah porta, jadi saya beranggapan untuk memecahkan pesan di atas kita bisa

menggunakan cipher porta, namun setelah di decode hasilnya huruf acak,

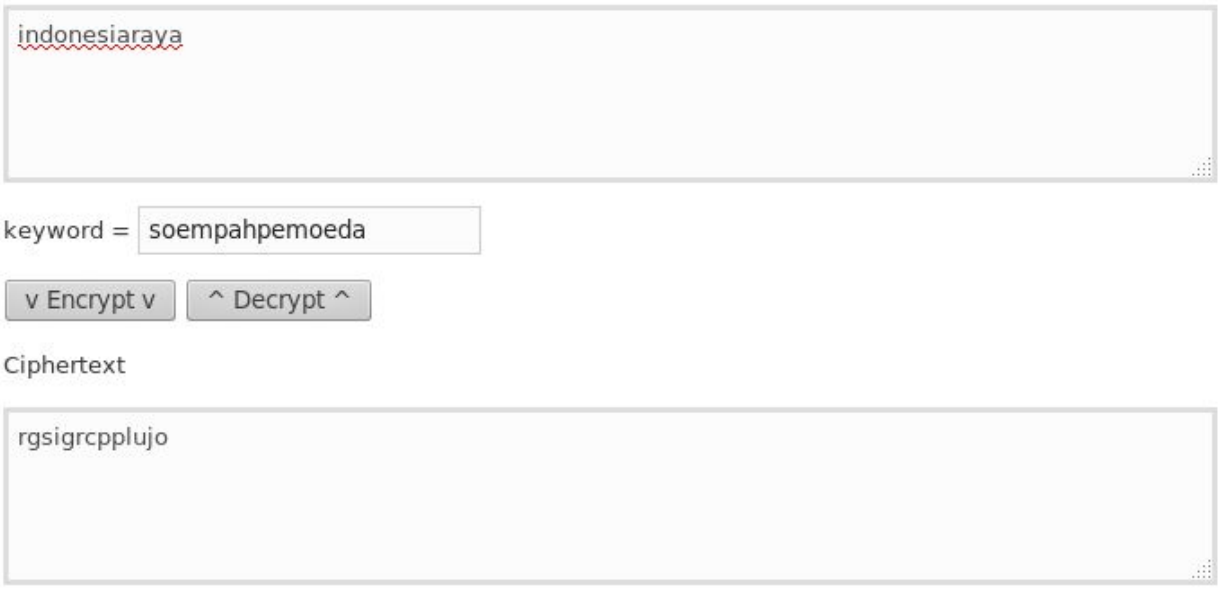


Namun setelah di analisa key di atas masih di encrypt menggunakan cipher ROT13.

ROT13 (dari Bahasa Inggris rotate by 13, putar 13 kali), adalah algoritma enkripsi sederhana yang menggunakan sandi abjad-tunggal dengan pergeseran k=13 (huruf A diganti dengan N, huruf B diganti dengan O, dan seterusnya). Enkripsi ini merupakan penggunaan dari sandi Caesar dengan geseran 13. ROT13 biasanya digunakan di forum internet, agar spoiler, jawaban teka-teki, kata-kata kotor, dan semacamnya tidak terbaca dengan sekilas.(sumber : wikipedia)

```
root@joe:/# echo "fbrzcnucrzbrqn" | tr a-zA-Z n-za-mN-ZA-M
soempahpemoeda
root@joe:/#
```

Setelah di decode di dapat bahwa key yang sebenarnya adalah “soempahpemoeda”, sekarang kita coba decode menggunakan key “soempahpemoeda” dengan cipher porta.



Upss.. Cipher telah berhasil kita pecahkan, plaintextnya adalah “indonesiaraya”

7. *Conclusion*

Flag : COMNETS{indonesiaraya}

8. *Reference*

http://practicalcryptography.com/ciphers/classical-era/porta/
https://id.wikipedia.org/wiki/ROT13