

Laporan Penyisihan 2 – Gemastik 8 Jaringan



Dibuat oleh : Psycho Security

Anton Salim (672011055)

Aditya Wicaksana (672012226)

Dhimas Wiharjo (672011205)

Fakultas Teknologi Informasi

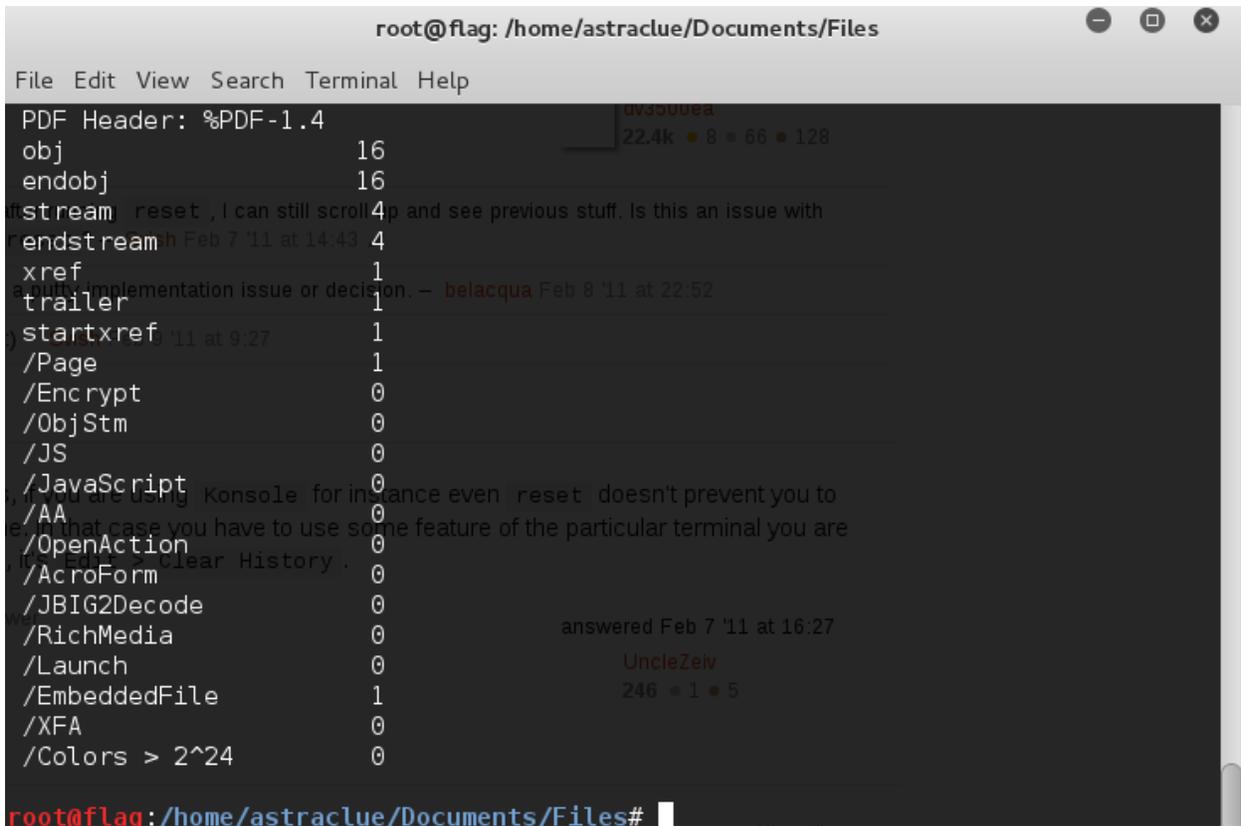
Universitas Kristen Satya Wacana

Soal A

Pada soal ini kita mendapatkan 5 buah file pdf.

```
root@flag:/home/astracloe/Documents/Files# ls
file1.pdf file2.pdf file3.pdf file4.pdf file5.pdf
root@flag:/home/astracloe/Documents/Files#
```

Terdapat file1.pdf, file2.pdf, file3.pdf, file4.pdf, dan file5.pdf.



```
root@flag: /home/astracloe/Documents/Files
File Edit View Search Terminal Help
PDF Header: %PDF-1.4
obj 16
endobj 16
stream reset , I can still scroll up and see previous stuff. Is this an issue with
endstream Feb 7 '11 at 14:43 4
xref 1
trailer 1
startxref Feb 7 '11 at 9:27 1
/Page 1
/Encrypt 0
/ObjStm 0
/JS 0
/JavaScript 0
/AA 0
/OpenAction 0
/AcroForm 0
/JBIG2Decode 0
/RichMedia 0
/Launch 0
/EmbeddedFile 1
/XFA 0
/Colors > 2^24 0
root@flag:/home/astracloe/Documents/Files#
```

Kita menggunakan pdftotext dan ternyata ada file embed di dalam file tersebut.

Oleh sebab itu kami gunakan pdftk untuk uncompress file yg ada di pdf1 sampai pdf5 menjadi sebagai berikut :

```
root@flag: /home/astracloe/Documents/Files
File Edit View Search Terminal Help
root@flag: /home/astracloe/Documents/Files# ls
data1.pdf data3.pdf data5.pdf file2.pdf file4.pdf
data2.pdf data4.pdf file1.pdf file3.pdf file5.pdf
root@flag: /home/astracloe/Documents/Files#
```

Setelah itu kami buka hasilnya maka akan terlihat beberapa hash yang terdapat di dalam file – file pdf tersebut :

Clue pdf1 ada hash sebagai berikut “33e75ff09dd601bbe69f351039152189”.

```
root@flag: /home/astracloe/Documents/Files
File Edit View Search Terminal Help
%PDF-1.4
1 0 obj
/Size 73
endobj
2 0 obj
/Type /EmbeddedFile
/Params 1 0 R
/Length 73
stream
Bagian pertama.
Dari mana datangnya 33e75ff09dd601bbe69f351039152189 ?
endstream
endobj
3 0 obj
/Type /F
/F (data1.txt)
/UF (
/EF
/F 2 0 R
endobj
4 0 obj
/Names [(
t) 3 0 R]
:
```

Clue pdf 2

Bagian Dua.

Dari mana datangnya ea0f3b9271eff45033bea3a6b1c36fa0000c3de7 ?

Clue pdf 3

Bagian Tiga.

Dari mana datangnya a9bcf1e4d7b95a22e2975c812d938889 ?

Clue pdf 4

Bagian Empat.

Dari mana datangnya 1489eec1dd6f153d2da7d5a4b40bc078896fc006c8534dc449ce35e28436fd6a ?

Clue pdf 5

Bagian Terakhir.

Dari mana datangnya 44c582df70cc6e653adf2cf0df3f29fd1b6e16ca ?

Setelah kami analisis sepertinya menggunakan hash clue nya maka saya check dengan hash-identifier untuk menyakinkan kembali ternyata benar menggunakan hash.

Hash 1 : md5

Hash 2 : sha1

Hash 3 : md5

Hash 4 : sha256

Hash 5 : sha1

Kami menggunakan decoder online sesuai hash yang digunakan seperti md5hasing.net atau hashkiller.co.uk untuk mendeskripsikan maksud clue tersebut.

Q	Search
#	Hash Type Checker
🔒	Crypter
✉	Anonymous Email
💬	Crypto Chat
🗨	Open Chat
🔑	Password Generator
☰	Last Queries List

Reverse decryption: Searching for 33e75ff09dd601bbe69f351039152189

Decoded Value:

28

Select Decoded Value

Your hash is decoded! You're very lucky

Hash type: md5

Hasilnya sebagai berikut :

Clue 1 : 28

Clue 2 : okt

Clue 3 : hari

Clue 4 : sumpah

Clue 5 : ...?

Kalo melihat dari cluenya yang sudah ditemukan akan menjadi **28 okt hari sumpah ... ?**

Awalnya kita tidak menemukan clue 4, kita mencoba submit dengan “sumpahpemuda” berulang – ulang, ternyata jawabannya hanya “pemuda”.

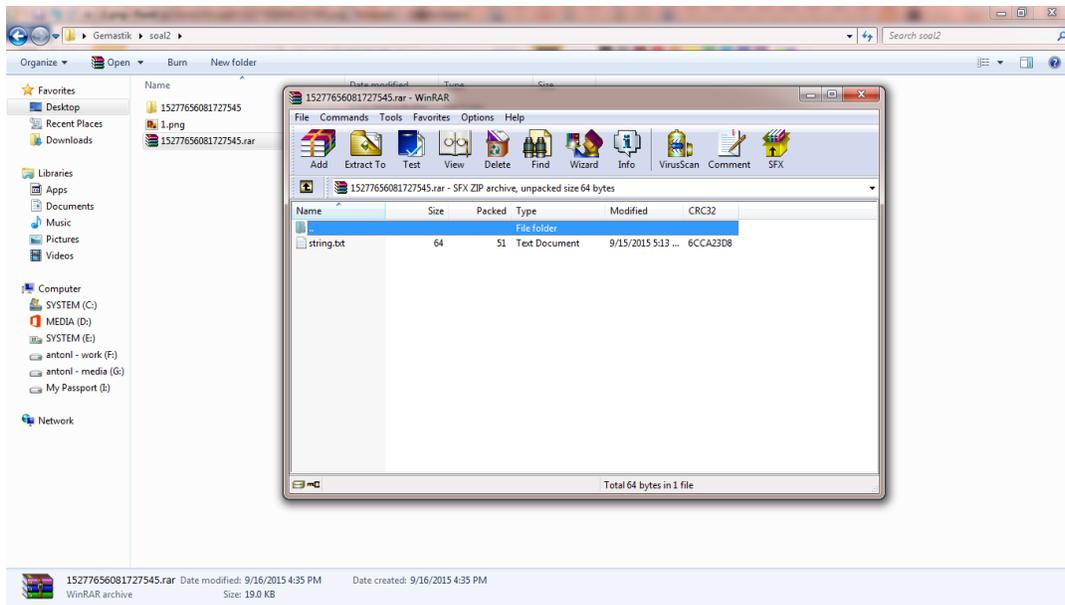
Soal B



Dalam soal ini kita diminta untuk mengunduh file gambar yang bernama “15277656081727545.png”. Karena tidak ada clue lain, kita mencoba membukanya dengan notepad file tersebut.

```
D:\Users\Documents\User\Desktop\Gemastik\soal2\15277656081727545.png - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
15277656081727545.png
97  òè
98  STXGS±P;Â´'è
99  NUL!ò´ ò+Lc×4STXGSβòDC3ÓFVHWNULBS0½G0A>, @ ĐqŠo¼DC2 {EOTİã+I
100 NULeHi) fMÇĐNAKáÇ; òðĐJM; -Ø {öWLK¥KNUL"Nx»ÖEOTùx°, DC1: üfUS@} EC
101 DC3XNULDC4ÇCANiĐ±š@ ĐDC1ESúÈìVÓ. DC3ö$ACKpj¹Đ½â&aßBSSTXGSöŽ
102 NULESòì çy÷BSDLEèBS`#šö~lENO] SOHDÚ
103 i^ðDLE]A #¼SYNHlACKèH°STX^¤FTB¼{ÀSTX°, @GøiMæ;M»DxÔACKDÅfi3ÿ
104 kË t8-xûÆĐox·SO, f...÷Ûp;°|•@SVT" cŠĂĐ«iíæB°ETXBSµBi³ÜÑûlETXRá
105 sM%ö8ž°ð@ü?fzÿÁ`ÂâuDLEè(%)İªDC3ætIÌD°ETX^<%Đ^ünaM9BSt"1}İ7Øl
106 ½İEOTû%e@GhGiú~P'İ
107 DC1¶vDtLñ@ù¶Đg€DC19BS±8c, ÄjÄw`Ø1^&SOHÁ5zM;ê]ãý¼kRS Đá, Ý;Y×Û
108 ¼kiACKiš»Ó»ACKPI¤VTIDLE`Zæ¬¥™6Ô'+M»Đ'EOT°BEL¥FFqÝálæiãEM...f(
109 ñ7M{Ç´ES°ETXEOT:à/¼DC1òZ+ETBiSUBðETXéSUBæÀ$/À5ÈÛkNULÎªpiØ±
110 NULNULNULstring.txtENOÁ%DC1À0BSETX°•LÊK=Žy²ÿBS•NGSRfµ#NULİ
111 NULNULNULNULNULNULNULSOHNUL NULNULNULNULNULNULNULstring.t.
Normal text file length:19480 lines:111 Ln:110 Col:14 Sel:10|0 Dos:Windows ANSI INS
```

Disini kita melihat di baris 110, kita mencurigai ada file “string.txt”.



Setelah mencobanya kita mengubah format file beberapa kali, ternyata file .rar lalu kita extract file tersebut dan menemukan file string.txt



Isi dalam file string.txt berupa hash
“2b299a11beda0003372f849ce5a9919c3eeaae70094b45f5a05d0ad5da49aac9”.

HASH TYPE CHECKER · MD2 · MD4 · MD5 · SHA1 · SHA224 · SHA256 · SHA384 · SHA512 · RIPEMD128 · RIPEMD160 · RIPEMD256 · RIPEMD320 · WHIRLPOOL · TIGER128,3 · TIGER160,3 · TIGER192,3 · TIGER128,4 · TIGER160,4 · SNEFRU · SNEFRU256 · GOST · ADLER32 · CRC32 · CRC32B · FNV132 · FNV164 · JOAAT · HAVAL128,3 · HAVAL160,3 · HAVAL192,3 · HAVAL224,3 · HAVAL256,3 · HAVAL128,4 · HAVAL160,4 · HAVAL192,4 · HAVAL224,4 · HAVAL256,4 · HAVAL128,5 · HAVAL160,5 · HAVAL192,5 · HAVAL224,5 · HAVAL256,5 · MD5X2 · MD5X3 · MD5X4 · MD5X5 · PASSWORD GENERATOR · DATA CRYPTER · ANONYMOUS CRYPTO CHAT · ANONYMOUS OPEN CHAT · ANONYMOUS DISPOSABLE EMAIL

Reverse decryption: Searching for 2b299a11beda0003372f849ce5a9919c3eeaae70094b45f5a05d0ad5da49aac9?is_search=true#main

Decoded Value:
kamiagenperubahan

Select Decoded Value

Your hash is decoded! You're very lucky

Hash type: gost

Search hash: 2b299a11beda0003372f849ce5a9919c3eeaae70094b45f5a05d0ad5da49aac9

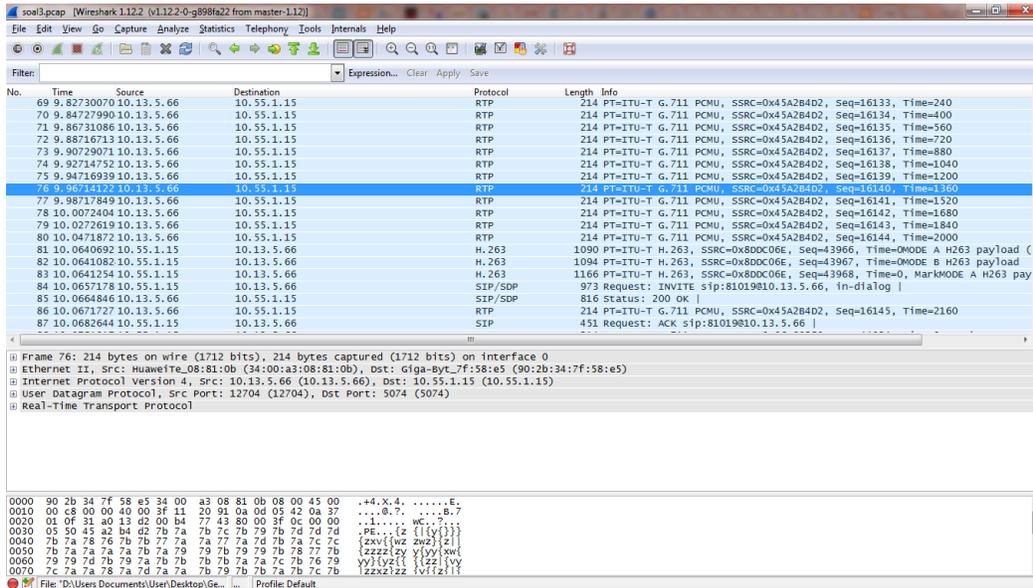
md2	md4
md5	sha1
sha224	sha256
sha384	sha512

All hashes:

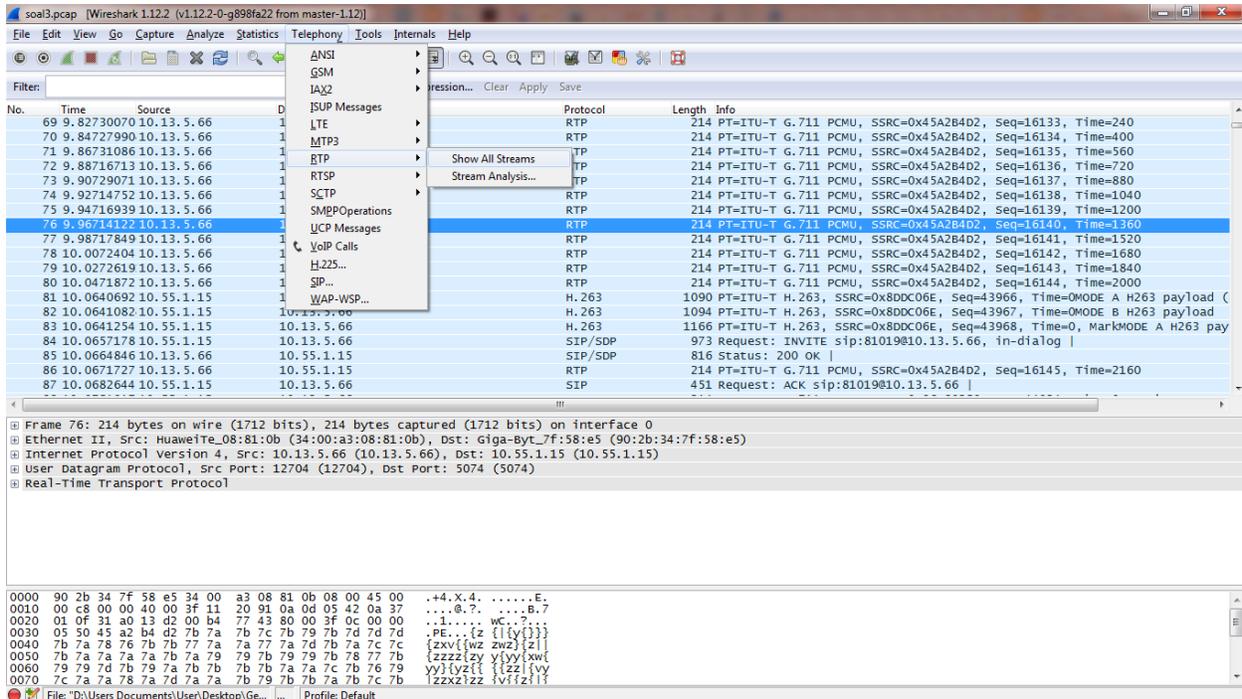
Select Hash: **md2** 0debfd737694b7a9b64aa92fca967b21

Kita menyelesaikan dengan menggunakan tools online “md5hashing.net” untuk memecahkannya dan ternyata setelah di decode diketahui jawabannya “kamiagenperubahan” yang merupakan hasil dari hash type : gost.

Soal C



Pada soal ini kami mendapatkan file “soal3.pcap”, setelah dibuka dengan wireshark kita melihat ada banyak protocol RTP.



Kita mencoba membuka streams untuk mencari tahu apakah ada percakapan yang terjadi dalam soal file .pcap ini. Telephony > RTP > Show All Streams.

The screenshot shows the Wireshark interface with the following components:

- Packet List:** A table of captured packets, primarily RTP, showing source and destination IP addresses and ports.
- Wireshark: RTP Stream Analysis:** A dialog box showing analysis statistics for a selected RTP stream. It includes a table of packet statistics and summary metrics like Max delta, Max jitter, and Total RTP packets.
- Wireshark: RTP Streams:** A dialog box listing detected RTP streams with columns for source/destination addresses, ports, SSRC, payload, and packet counts.
- RTP Player:** A window for playing back the RTP stream, showing a waveform and playback controls like 'Play', 'Pause', and 'Stop'.

Setelah itu kami menemukan ada file yang bisa di analyze, kita mencoba membuka file tersebut dan ada pesan angka yang disampaikan “2810192828102015”. Angka tersebut merupakan jawaban dari soal ini.

Soal E

Pada soal ini kita mendapatkan clue “fun crypto”, dan ternyata ada 3 baris dan memiliki berbeda jenis.

Geser sedikit dong ...

Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdpd gdul nxqfl dgdodk "uxgqx", wdqsd wdqgd shwln.

Butuh kunci untuk membuka pesan.

lyek iuo 1000 btixa gwi, xcfeiu nmix eheilg umwyew lklv csklaai. lyek iuo 10 cguexn pqcwnai kenp seahpkkhtmix xhpqk. vniqkh xgleu qczs ehpkv uqctkb "zivknacx", duari duafi zygks

Bekerja keras untuk memenuhi kebutuhan keluarga (diperibahasakan)

Yztrzm gvizpsri wzir pfmxr zwzozs "hfivgfqzn" gzmzkz gzmwz kvgrp.

Caesarian Shift
Rumkin.com >> Web-Based Tools >> Ciphers and Codes

This is a standard Caesarian Shift cipher encoder, also known as a rot-N encoder and is also a style of substitution cipher. This way, you can add one, two, or any number up to 25 to your string and see how it changes. This is an offshoot of the [rot13](#) encoder on this web site. To perform this shift by hand, you could just write the alphabet on two strips of paper. Line them up so the top strip's A matches the bottom strip's D (or something) and then you can encode. A simple test to see how this works would be to [insert the alphabet](#) into the encoder and then change the values of N.

This sort of cipher can also be known as a wheel cipher. This is where an inner wheel has the alphabet around the outside, and that is placed upon an outer wheel, also with the alphabet going around it. You can rotate the wheels so that ABC lines up with ABC, or ABC may line up with QRS.

To encode something, just pick an N and type in your message. To decode something, subtract the encryption N from 26 and it should be decoded for you.

N:

Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdpd gdul nxqfl dgdodk "uxgqx", wdqsd wdqgd shwln.

This is your encoded or decoded text:

Pemuda indonesia yang berbahagia. Kita adalah generasi penerus bangsa. Bagian pertama dari kunci adalah "rudnu", tanpa tanda petik.

Amadillos bury their excrement in a manner similar to cats. Tyler Akins <tidian@rumkin.com> Contact Me - Legal Info

Pada baris pertama kita mengerjakan menggunakan tools online dari rumkin.com

“Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdpd gdul nxqfl dgdodk "uxgqx", wdqsd wdqgd shwln.” Merupakan Caesarian Shift yang digeser 23.

Hasilnya “Pemuda indonesia yang berbahagia. Kita adalah generasi penerus bangsa. Bagian pertama dari kunci adalah "rudnu", tanpa tanda petik.”

rumkin.com/tools/cipher/vigenere-keyed.php

Keyed Vigenere Cipher

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

Based on the simpler [Vigenere](#) cipher, this uses an alternate tableau. The "Alphabet Key" helps decide the alphabet to use to encrypt and decrypt the message. The "Passphrase" is the code word used to select columns in the tableau. Instead of just using the alphabet from A to Z in order, the alphabet key puts a series of letters first, making the cipher even tougher to break. This style of encryption is also called a Quagmire III.

This tool was built to play with the [Kryptos](#) codes – a set of letters that are cut out of a sheet of copper at the CIA headquarters. To help you out with the codes, you can pre-populate the form with the [K1](#) or [K2](#) sections. Also, there is a [Corrected K2](#) that shows where a letter was omitted (the lower-case "s" near the end).

Decrypt ▾

Alphabet Key: - [Show Keymaker](#)

Alphabet Used: ABCDEFGHIJKLMNOPQRSTUVWXYZ - [Show Tableau](#)

Passphrase:

Your message:

```
lyek iuo 1000 btixa gwi, xcfeiiu nmix eheilog umwyew lklv csklaai. lyek iuo 10 cguexn pqcwnai
kenp seahpkkhtmix xhpkq. vniqkh xgleu qczs ehpkq uqctkb "zivknacx", duari duafi zygks
```

This is your encoded or decoded text:

```
beri aku 1000 orang tua, niscaya akan kucabut semeru dari akarnya. beri aku 10 pemuda niscaya akan kuguncangkan dunia. bagian kedua dari kunci adalah "mgnatnap", tanpa
tanda petik
```

INDEX

- Affine
- Atbash
- Baconian
- Base64
- Bifid
- Cæsar
- Keyed
- ROT13
- Column Trans.
- Double
- Ubcii
- Cryptogram
- Gronsfeld
- Morse
- Numbers
- One Time Pad
- Playfair
- Railfence
- Rotare
- Skip
- Substitution
- Vigenere
- Keyed
- Autokey
- Crypto Solver
- Frequency
- Manipulator

Weigh your ideas carefully, they may make you rich.

Tyler Akins <tidian@rumkin.com>
[Contact Me](#) - [Legal Info](#)

Pada baris kedua “lyek iuo 1000 btixa gwi, xcfeiiu nmix eheilog umwyew lklv csklaai. lyek iuo 10 cguexn pqcwnai kenp seahpkkhtmix xhpkq. vniqkh xgleu qczs ehpkq uqctkb "zivknacx", duari duafi zygks” yang merupakan Keyed Vignere Ciphere dan kita mendapatkan clue “butuh kunci untuk membuka pesan”.

Hasilnya “beri aku 1000 orang tua, niscaya akan kucabut semeru dari akarnya. beri aku 10 pemuda niscaya akan kuguncangkan dunia. bagian kedua dari kunci adalah "mgnatnap", tanpa tanda petik” di decrypt dengan Passphrase “kunci”.

Pada baris ketiga “Yztrzm gvizpsri wzir pfmxr zwzozs "hfivgfqzn" gzmzk gzmwz kvgrp.” yang merupakan Atbash Cipher. Setelah di decode “Bagian terakhir dari kunci adalah "suretujam" tanpa tanda petik.”.

```

Untitled - Notepad
File Edit Format View Help
Geser sedikit dong ...

Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdf
Pemuda indonesia yang berbahagia. Kita adalah generasi penerus bangsa. Bagian pertan
Butuh kunci untuk membuka pesan.

kunci
lyek iuo 1000 btixa gwi, xcfeiiu nmix eheilog umwyew lklv csklaai. lyek iuo 10 cgue)
beri aku 1000 orang tua, niscaya akan kucabut semeru dari akarnya. beri aku 10 pemu

Bekerja keras untuk memenuhi kebutuhan keluarga (diperibahasakan)

Yztrzm gvizpsri wzir pfmxr zwzozs "hfivgfqzn" gzmzk gzmwz kvgrp.
Bagian terakhir dari kunci adalah "suretujam" tanpa tanda petik.

"rudnumgnatnapsuretujam"

Kumpulkan jawaban dalam sebuah source code Python berekstensi (.py). Dua baris kode
soal5 = raw_input()
print('put your answer here') #Tuliskan jawaban diantara tanda petik

```

Dari hasil semua decode terdapat kata yang direverse dalam tanda “, kita coba gabungkan kita menemukan hasil “majuteruspantangmundur”. Setelah mencoba submit jawaban ternyata salah, tetapi jawabannya memang tetap reverse yaitu “rudnumgnatnapsuretujam”.