IF4020 Kriptografi

09 - Steganografi

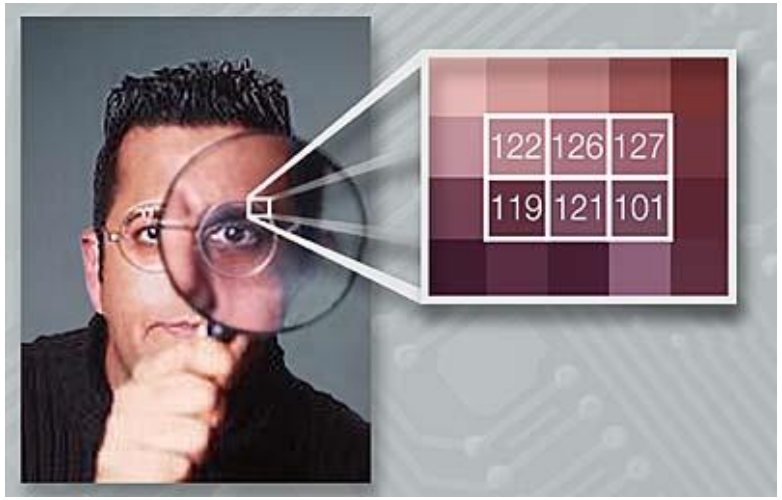
(Bagian 2)

Oleh: Rinaldi Munir

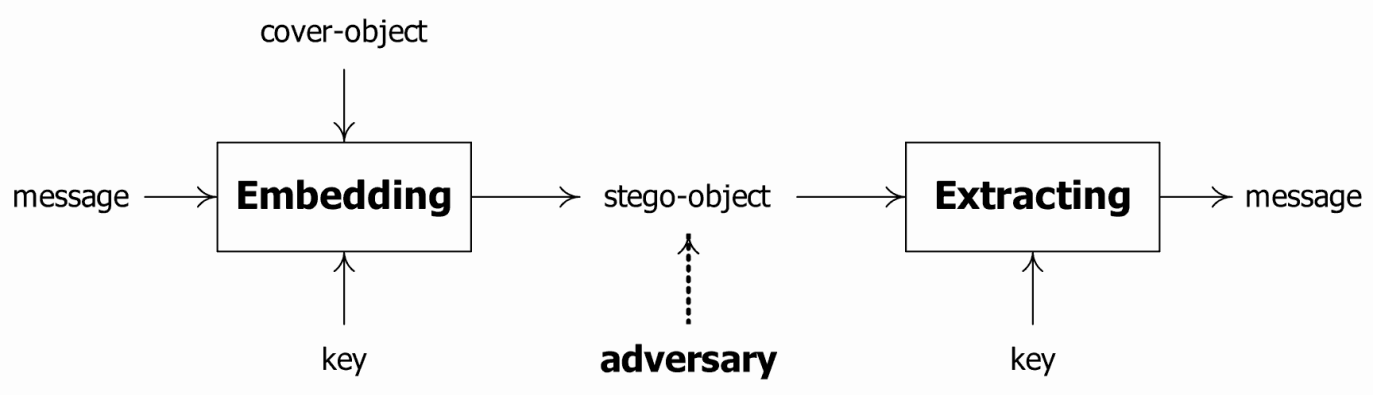
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
InstitutTeknologi Bandung
2023

Steganalysis

- Tujuan: menentukan apakah sebuah media *suspect* mengandung pesan tersembunyi



- Steganografi



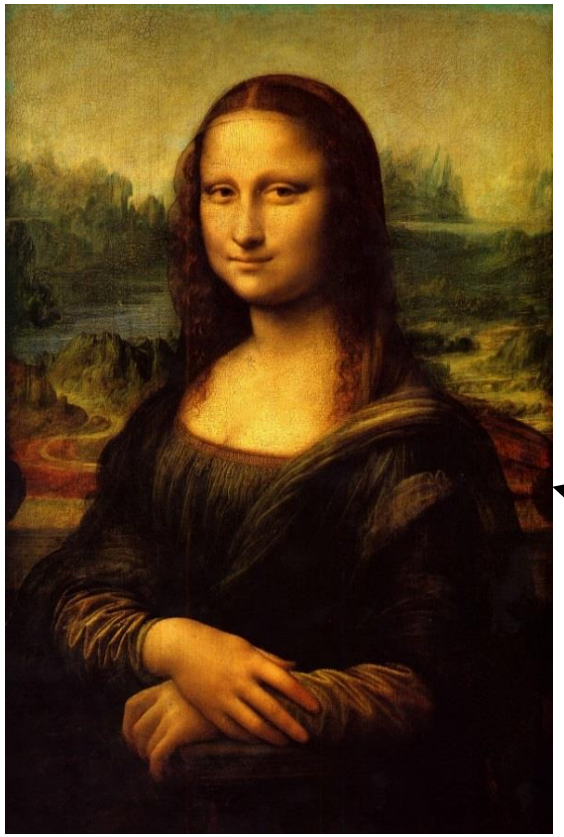
- Steganalisis

*) Keterangan: 1 jika ada pesan tersembunyi, 0 jika tidak

Fakta: Gambar-gambar bertebaran di internet

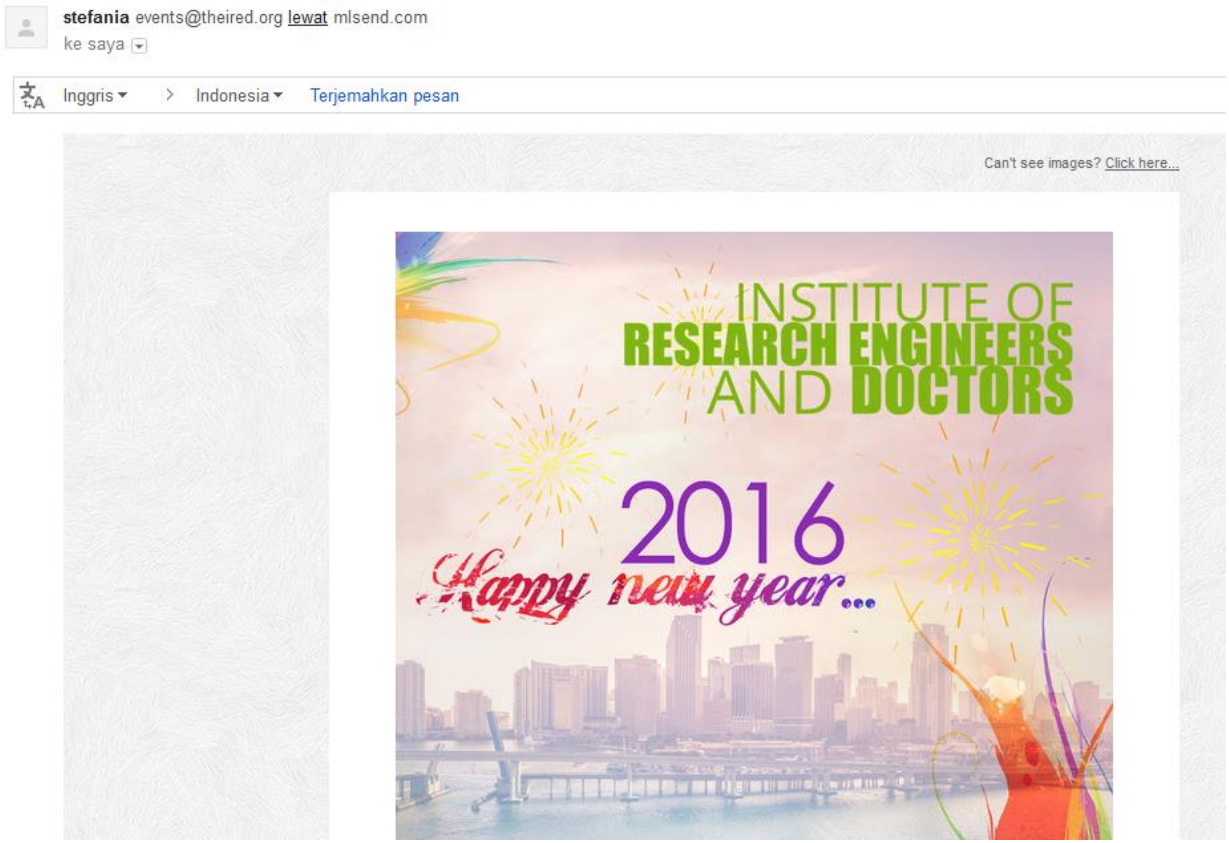
(*website*, *social media*, *social networking*)

Namun, dibalik sebuah gambar dapat tersembunyi informasi rahasia

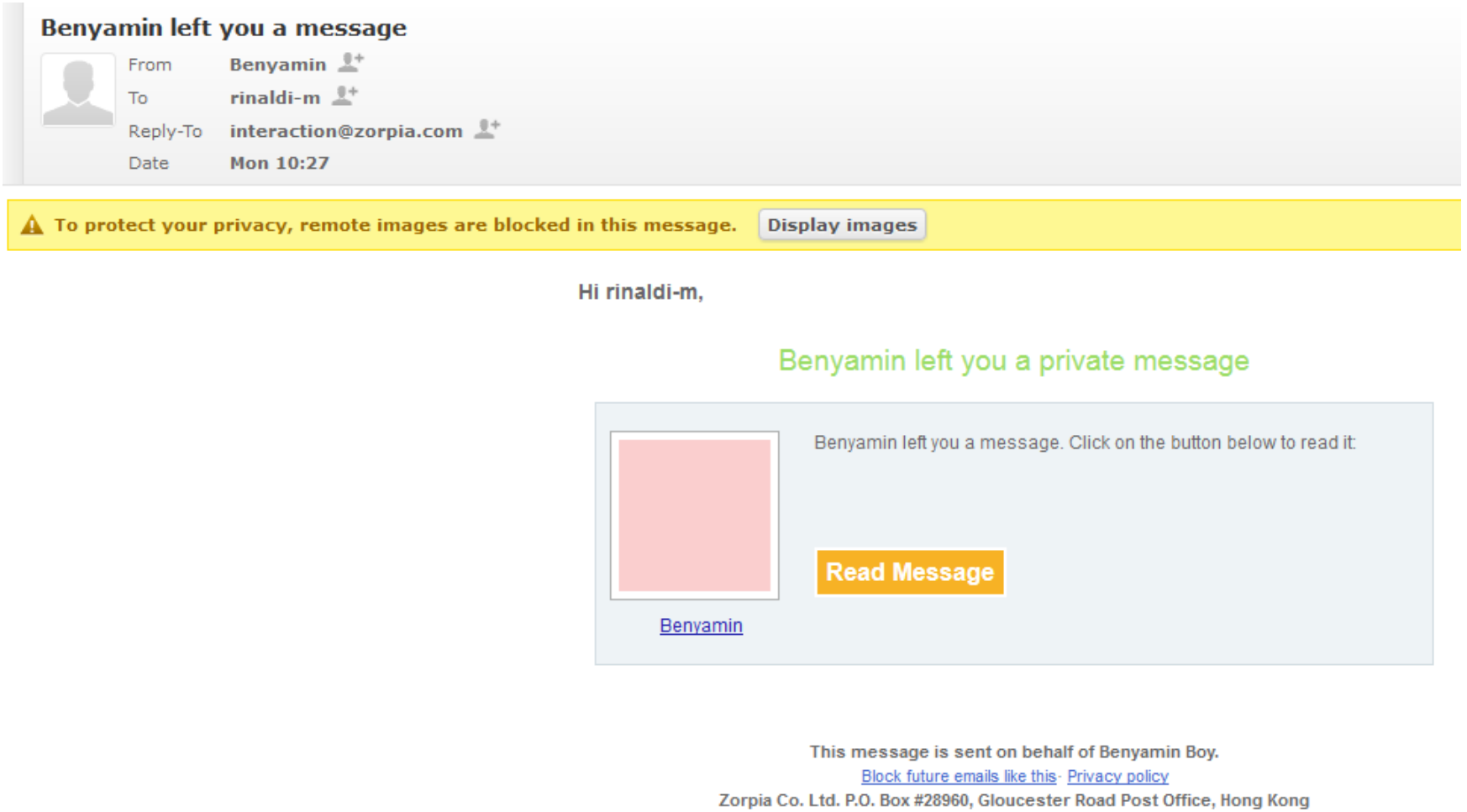


Informasi rahasia tersebut dapat berupa pesan biasa, pesan kejahatan, program jahat, bahkan virus komputer!

Pernah terima surel (*e-mail*) dari orang tak dikenal dan mengandung *file attachmet* berupa gambar seperti di bawah ini?



HATI-HATI!!!!!!!!!



HATI-HATI! Jangan langsung klik jika anda tidak yakin!

Ingat kembali stegosploit!!!

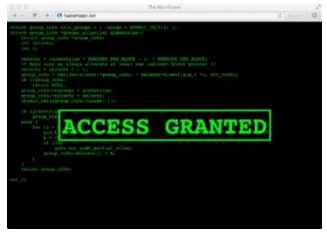
How to Hack a Computer Using Just An Image

Monday, June 01, 2015 Swati Khandelwal

Next time when someone sends you a photo of a cute cat or a hot chick than be careful before you CLICK on the image to view — it might hack your machine.

Yes, the normal looking images could hack your computers — thanks to a technique discovered by security researcher *Saumil Shah* from India.

Dubbed "***Stegosploit***," the technique lets hackers hide malicious code inside the pixels of an image, hiding a malware exploit in plain sight to infect target victims.



Just look at the image and you are HACKED!

http://thehackernews.com/2015/06/Stegosploit-malware.html

- Steganalisis diperlukan di dalam *forensic image analysis*

- ***Forensic Image Analysis*** *is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters.*

- Subdisiplin dari *Forensic Image Analysis:*

  (1) Photogrammetry

  (2) Photographic Comparison

  (3) Content Analysis

  (4) Image Authentication

- Salah satu pekerjaan di dalam *content analysis* adalah mendeteksi apakah ada pesan tersembunyi di dalam sebuah gambar.

- Contoh sebuah skenario: Mr. Abdul, seorang investigator forensik, diminta Lab Forensik Polri untuk menginvestigasi sebuah *cybercrime* berupa foto. Sebagai investigator forensik yang ahli, dia menganalisis foto untuk menemukan pesan tersembunyi di dalamnya dengan kakas steganalisis.

- Tujuan utama steganalisis adalah untuk membedakan apakah sebuah media mengandung pesan rahasia atau tidak.

- Steganalisis dianggap berhasil jika ia dapat menentukan apakah sebuah media mengandung pesan tersembunyi dengan peluang lebih tinggi daripada menerka secara acak.

- Selain tujuan utama di atas, terdapat beberapa tujuan minor steganalisis:

  - menentukan panjang pesan

  - menentukan tipe algoritma penyisipan

  - kunci yang digunakan

Jenis-jenis steganalisis

1. Targeted steganalysis

- Teknik steganalisis yang bekerja pada algoritma steganografi spesifik, dan kadang-kadang dibatasi hanya pada format media tertentu saja.

- Teknik ini mempelajari dan menganalisis algoritma penyisipan, lalu menemukan statistik yang berubah setelah penyisipan.

- Hasil steganalisis sangat akurat, tetapi tidak fleksibel karena tidak dapat diperluas untuk algoritma steganografi yang lain atau format media yang berbeda.

2. *Blind steganalysis*

- Teknik steganalisis yang bekerja pada sembarang algoritma steganografi dan sembarang format media.

- Teknik ini mempelajari perbedaan antara statistik *cover-object* dan *stego-object* dan membedakannya. Proses pembelajaran (*learning*) dilakukan dengan melatih (*training*) mesin pada sekumpulan database media. Model *machine learning* yang digunakan misalnya jaringan syaraf tiruan.

- Hasil steganalisis kurang akurat dibandingkan dengan teknik *targeted steganalysis*, tetapi kelebihannya adalah dapat diperluas untuk algoritma yang lain.

Metode Steganalisis

1 . **Serangan berbasis visual (*visual attacks*)**

- Khusus untuk *stego-object* berupa citra
- Bersifat subjektif, karena melakukan pengamatan secara kasat mata dengan melihat artefak yang mencurigakan di dalam *stego-image*, lalu membandingkannya dengan citra asli (cover *image*)
- Digunakan pada masa-masa awal riset steganalisis
- Contoh serangan visual:

  a. *LSB plane attack*

  b. *Filtered visual attack* (E*nhanced LSB*)

2. Serangan berbasis statistik (*statistical attack*)

- Menggunakan analisis matematik pada citra untuk menemukan perbedaan antara *cover image* dengan *stego image*.
- Didasarkan pada fakta bahwa penyembunyian pesan ke dalam media menimbulkan artefak yang dapat dideteksi secara statistik sehingga dapat mengungkap penyembunyian pesan atau pesan yang disembunyikan itu sendiri.
- Contoh serangan statistik:
  a. *histogram analysis*
  b. *Regular-singular* (RS) *analysis*
  c. *Chi-square analysis*
  d. *Sample pair* (SP) *analysis*

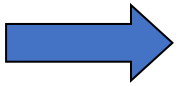
Visual Attack

- Memanfaatkan indera penglihatan → inspeksi kerusakan pada gambar akibat penyisipan

- Ide dasar :

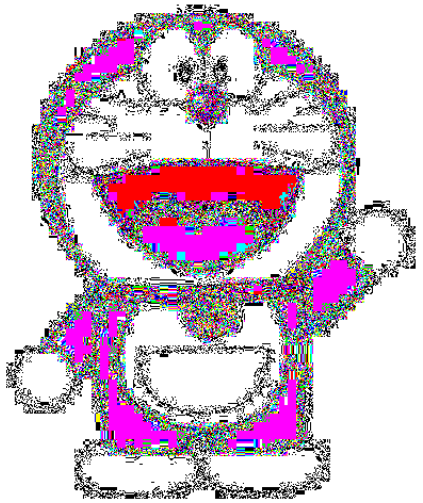
Metode Enhanced LSB

BLUE	GREEN	RED
1010010**1**	1001110**0**	1110011**1**



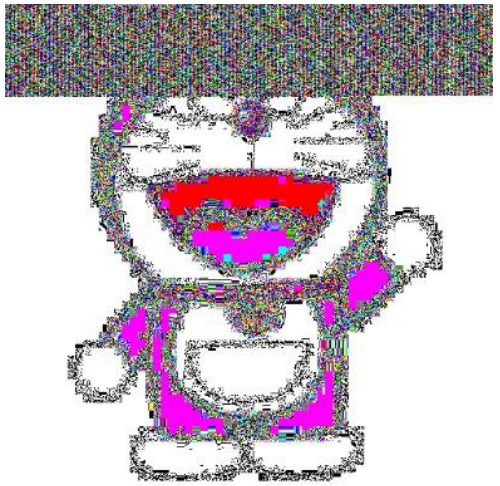
BLUE	GREEN	RED
11111111	**00000000**	**11111111**

(a) Citra orisinal



(b) Citra hasil *enhanced LSB*

(c) Citra stego



(b) Citra hasil *enhanced LSB*

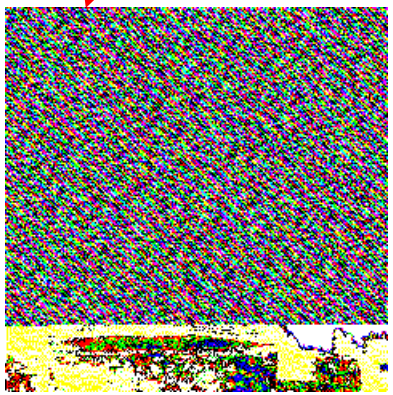
Teknik Steganalisis: *Visual Attack*

Artefak mencurigakan

Gambar asli

Hasil penapisan (asli)

Terdeteksi ada pesan



Terdeteksi ada pesan

Terdeteksi ada pesan

Terdeteksi ada pesan

Metode *enhanced-LSB* bagus untuk citra dengan kontras tinggi, yaitu citra yang memiliki warna latar yang jelas atau memiliki perbedaan warna yang kontras antara latar dengan gambar utama

Gambar III-1 Gambar yang mengandung pesan rahasia dan hasil *enhanced LSB*-nya [PAU07]

Untuk citra dengan kontras rendah (seperti citra hasil fotografi), metode *enhanced LSB* seringkali menyulitkan steganalis. Karena steganalis akan kesulitan membedakan antara gambar yang seharusnya muncul dengan pesan rahasia.

Gambar III-3 Gambar dengan kontras rendah dan hasil *enhaced LSB*-nya

NoStega: Noiseless Steganography

- Teknik baru steganografi, ditemukan oleh Desoky (2012)
- Tidak membutuhkan *cover* untuk menyembunyikan pesan
- Latar belakang: penyembunyian pesan di dalam *cover* dapat membuat kualitas *cover* menjadi terdegradasi ==> dapat diserang secara steganalisis untuk menemukan *embedded message*

- *NoStega* melakukan kamuflase dengan cara menyembunyikan pesan dalam bentuk *cover* yang terlihat alami sehingga tidak menimbulkan kecurigaan.

- *NoStega* menggunakan berbagai materi untuk melakukan kamuflase seperti grafik, email, game, catatan, dan lain-lain.

GraphStega (Graph Steganography)

- Salah satu teknik di dalam *NoStega*
- Melakukan kamuflase dengan cara mengubah pesan menjadi plot pada grafik.

- Contoh: pesan rahasia "*Use my secret key*".
  Ubah pesan ke dalam biner:

  01010101011100110110010100100000011011010111100100100000111001101100101011000110111100100110010101100000110101101100101011110010

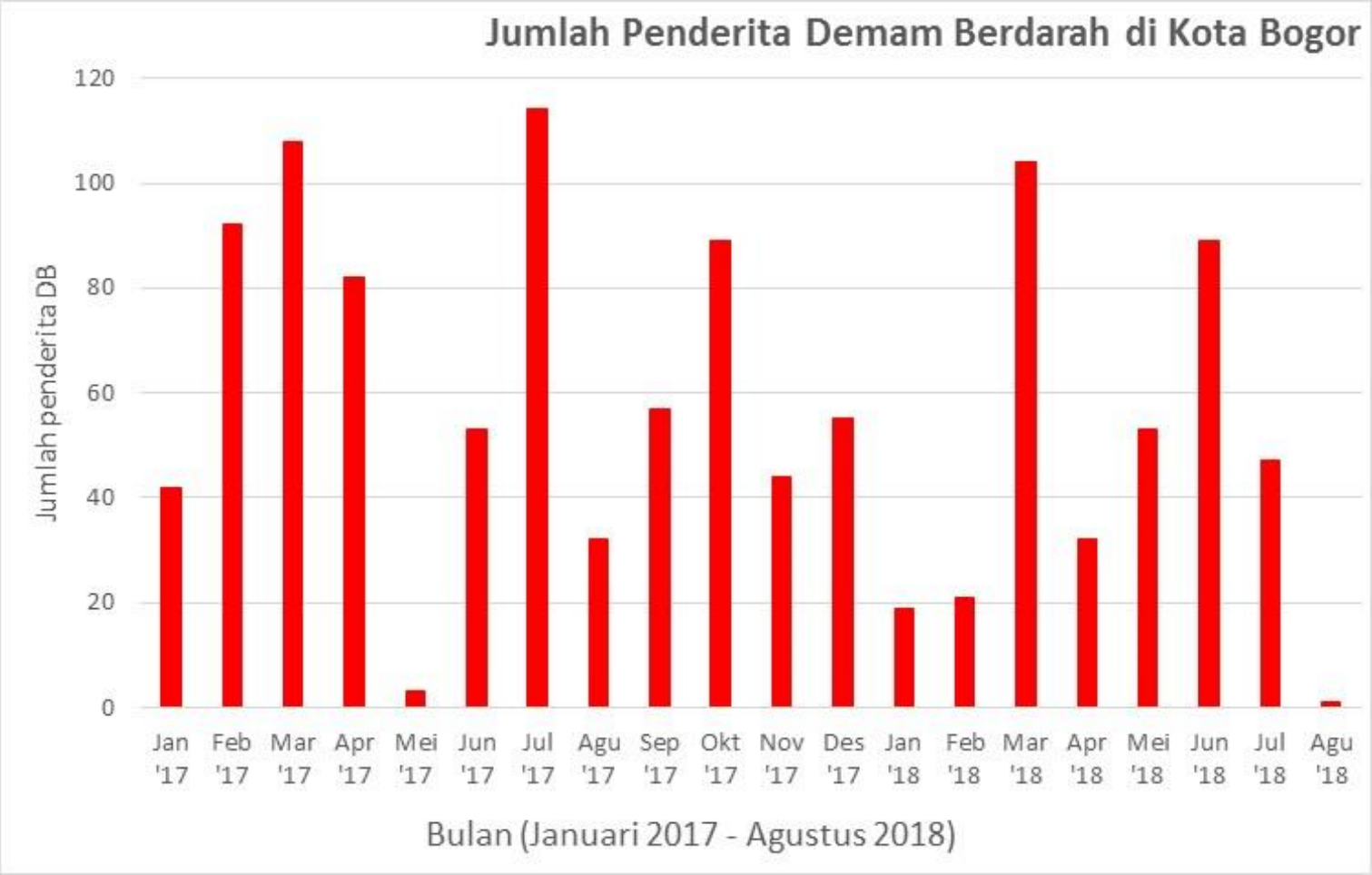
- Selanjutnya, kelompokkan menjadi kelompok-kelompok 7 bit:

0101010 1011100 1101100 1010010 0000011 0110101 1110010
0100000 0111001 1011001 0101100 0110111 0010011 0010101
1101000 0100000 0110101 1011001 0101111 001

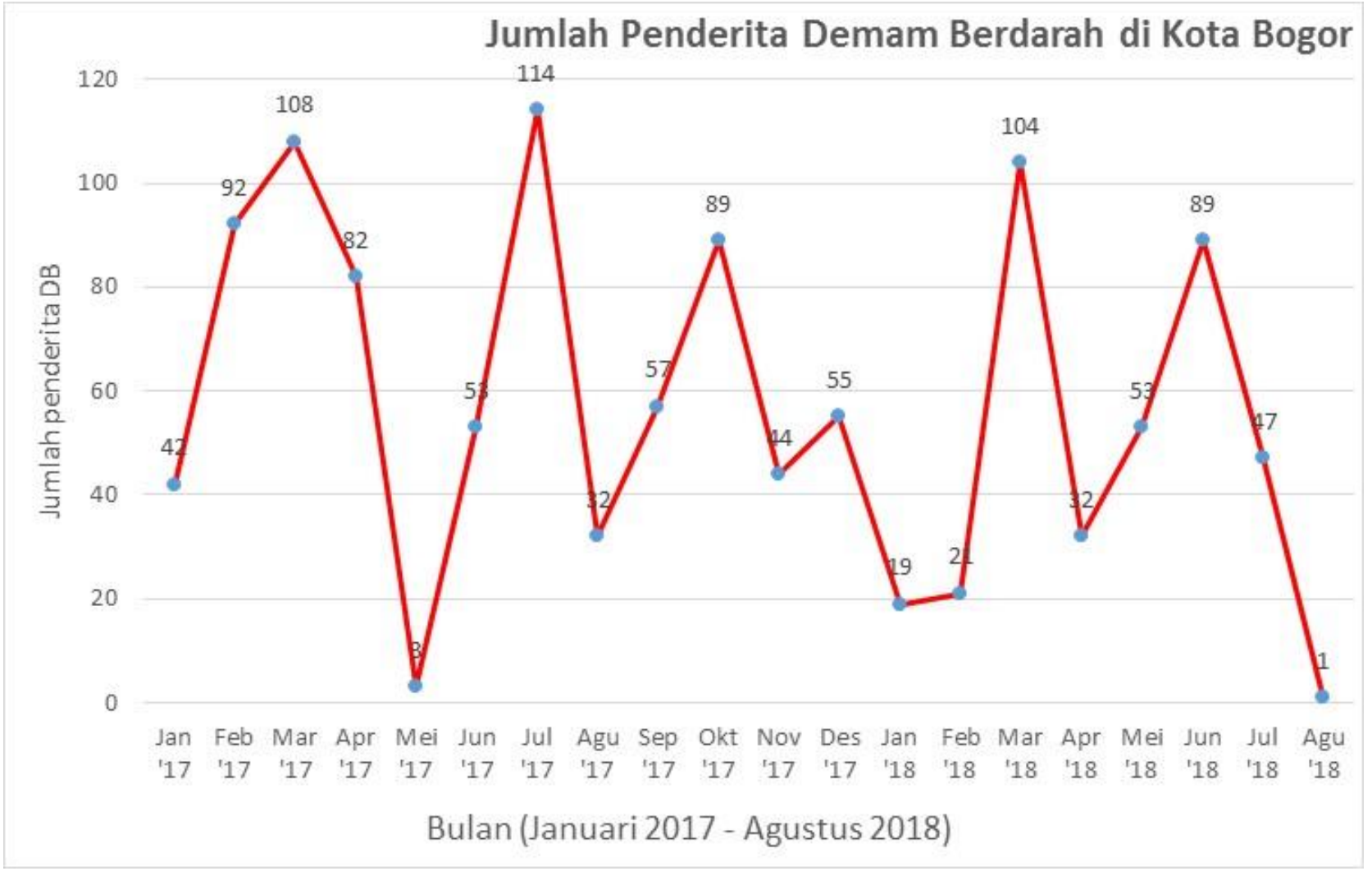
- Konversi kelompok-kelompok 7-bit di atas menjadi nilai desimal

42 92 108 82 3 53 114 32 57 89 44 55 19 21 104 32 53 89 47 1.

- Buatlah grafik dengan *Microsoft Excell* dengan menggunakan nilai-nilai desimal di atas
- Misalnya nilai-nilai tersebut menyatakan jumlah penderita demam berdarah selama 20 bulan di Kota Bogor (Januari 2017 – Agustus 2018).



Alternatif grafik lainnya:



Untuk membaca pesan rahasia, penerima membaca nilai-nilai pada grafik,

42 92 108 82 3 53 114 32 57 89 44 55 19 21 104 32 53 89 47 1

lalu mengubahnya ke dalam biner,

00101010 01011100 01101100 01010010 00000011 00110101 01110010
00100000 00111001 01011001 00101100 00110111 00010011 00010101
01101000 00100000 00110101 01011001 00101111 0001

Untuk setiap kelompok biner ambil 7-bit dari belakang (7-bit LSB),

0101010 1011100 1101100 1010010 0000011 0110101 1110010
0100000 0111001 1011001 0101100 0110111 0010011 0010101
1101000 0100000 0110101 1011001 0101111 001

Gabungkan semua kelompok bit menjadi satu,

010101010111001101100101001000000110110101111001001000001110011011001010110001101111001001100101011010000100000011010110110010101111001

Kemudian kelompokkan menjadi kelompok-kelompok 8-bit,

01010101 01110011 01100101 00100000 01101101 01111001
00100000 01110011 01100101 01100011 01110010 01100101
01110100 00100000 01101011 01100101 01111001

Kodekan setiap delapan bit tersebut menjadi karakter ASCII

Use my secret key

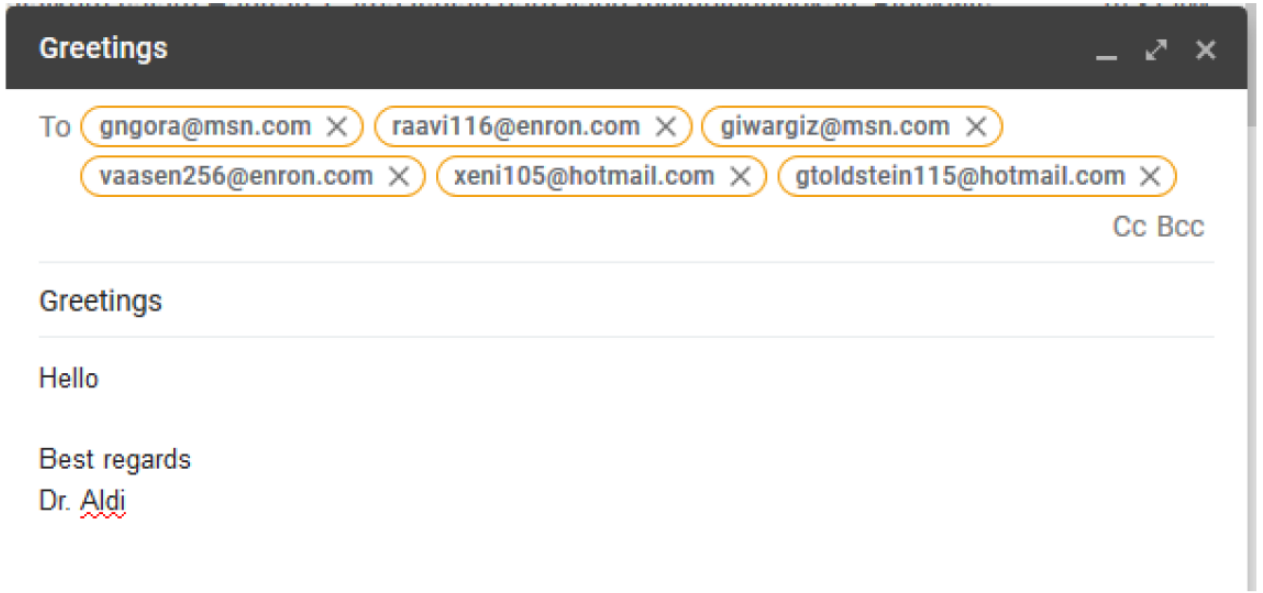
Pesan rahasia berhasil dibaca kembali!

Teknik NoStega lainnya

3. Nc3	Nf6
4. exd5	exd5
5. Nf3	Bd6
6. Bd3	O-O
7. O-O	h6
8. Re1	Nc6
9. Nb5	Bb4
10. c3	Ba5
11. Na3	Bg4
12. Nc2	Qd7
13. b4	Bb6
14. h3	Bh5
15. Ne3	Rfe8
16. b5	Ne7
17. g4	Bg6
18. Ne5	Qc8
19. a4	c6
20. bxc6	bxc6
21. Ba3	Ne4
22. Qc2	Ng5
23. Bxe7	Rxe7
24. Bxg6	fxg6
25. Qxg6	Nxh3+
26. Kh2	Nf4
27. Qf5	Ne6
28. Ng2	Qc7

The Chessmaster recommends: Queen to d3

Chess-stega



Head-stega

Ada pertanyaan?