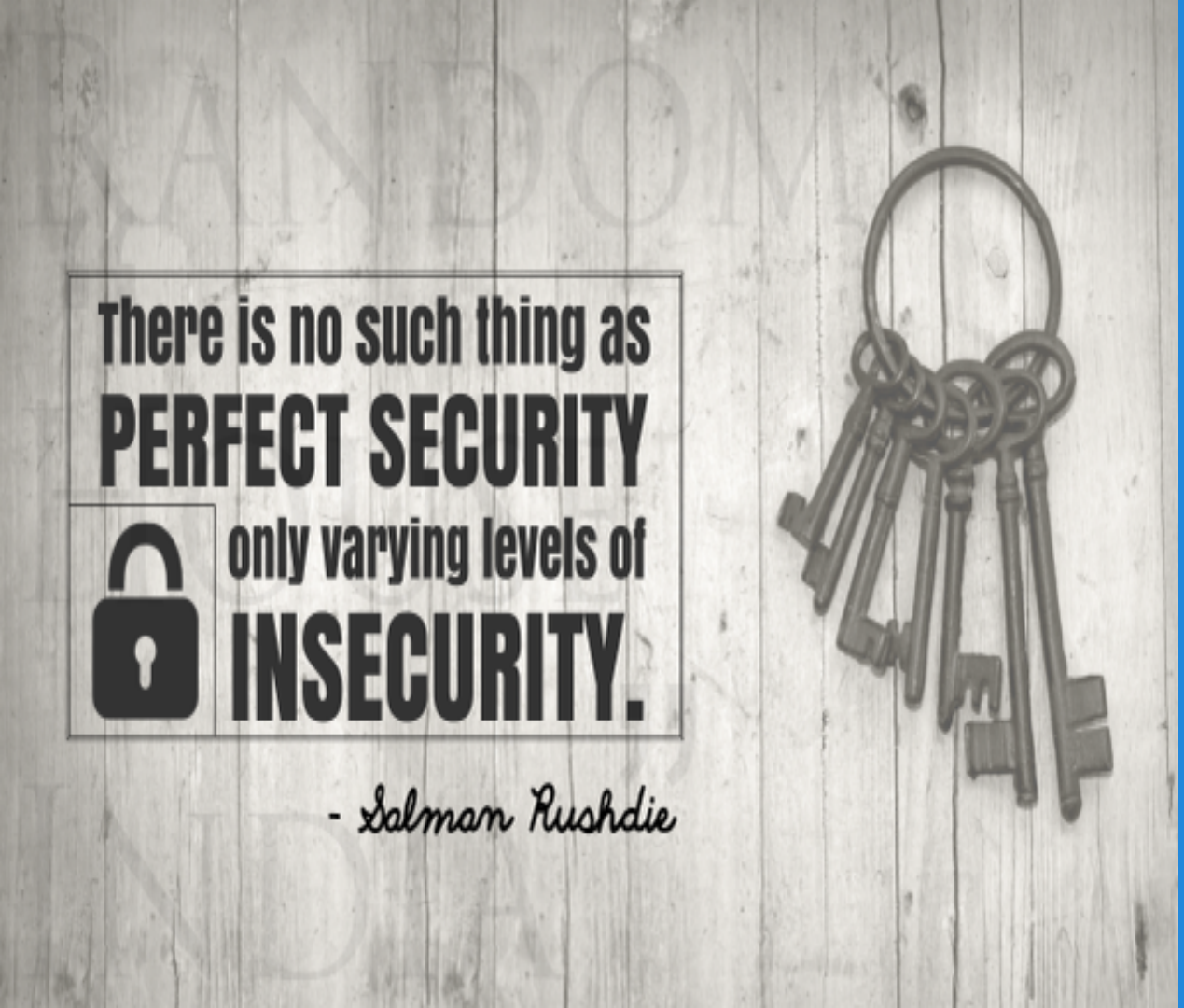
When will our Password be *Cracked ?!*

And how to choose strong password

1. *Adhika Setya P (42058)*
2. *Andika W.S (42060)*
3. *Edward (42095)*
4. *Elisabeth Diana K.S(42067)*
5. *M. Rifqi Zuliansyah (42054)*



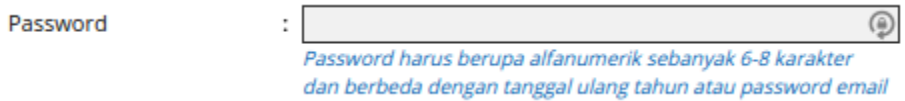
Semua sistem keamanan dapat dijebol!!!

Wait, what?

NAMUN hal yang bisa kita lakukan adalah menyandikan password dengan metode enkripsi sehingga cracker **membutuhkan waktu yang lama** untuk menebak password kita dengan cara brute force.

Website Owner Response

They restrict and force user to create a password that… must have number, minimal character, special character, etc.



Screenshot from one of the biggest bank with internet banking in Indonesia. This is their registration page.

Why? Because Password Entropy!

Bigger character pool + longer password

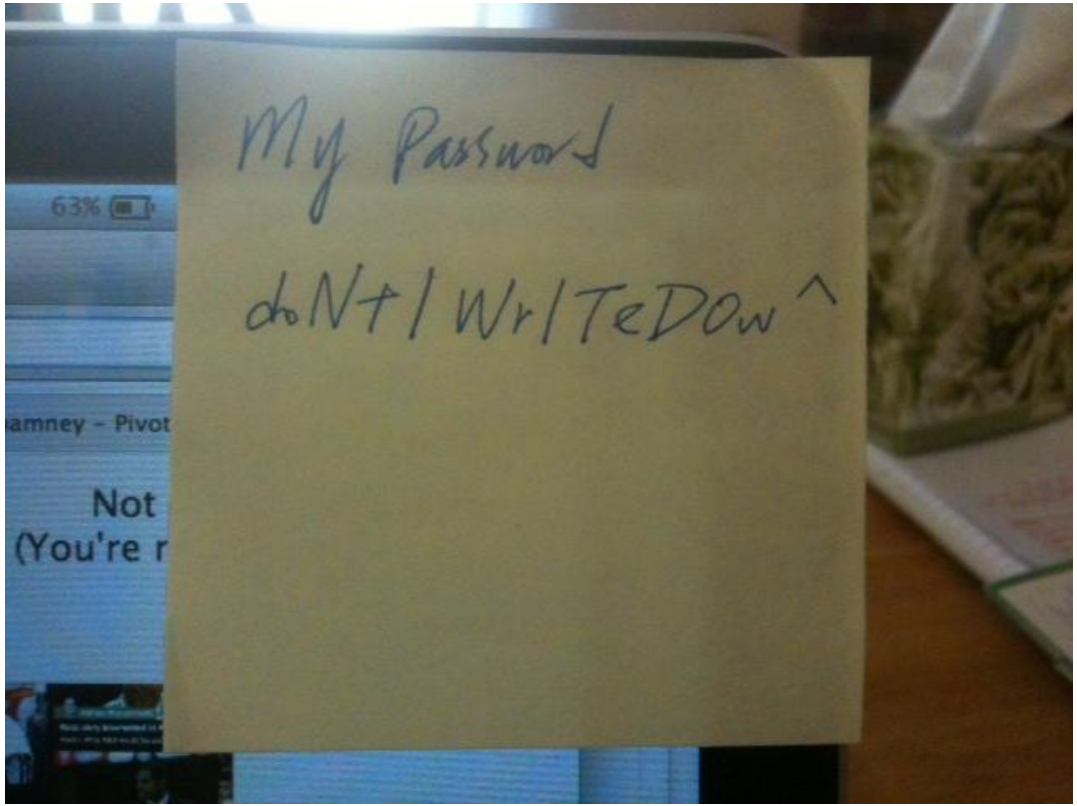
=

Bigger combination possibility

=

Longer time to crack

User (read: our) **Response**



Or using same password for **every** site.

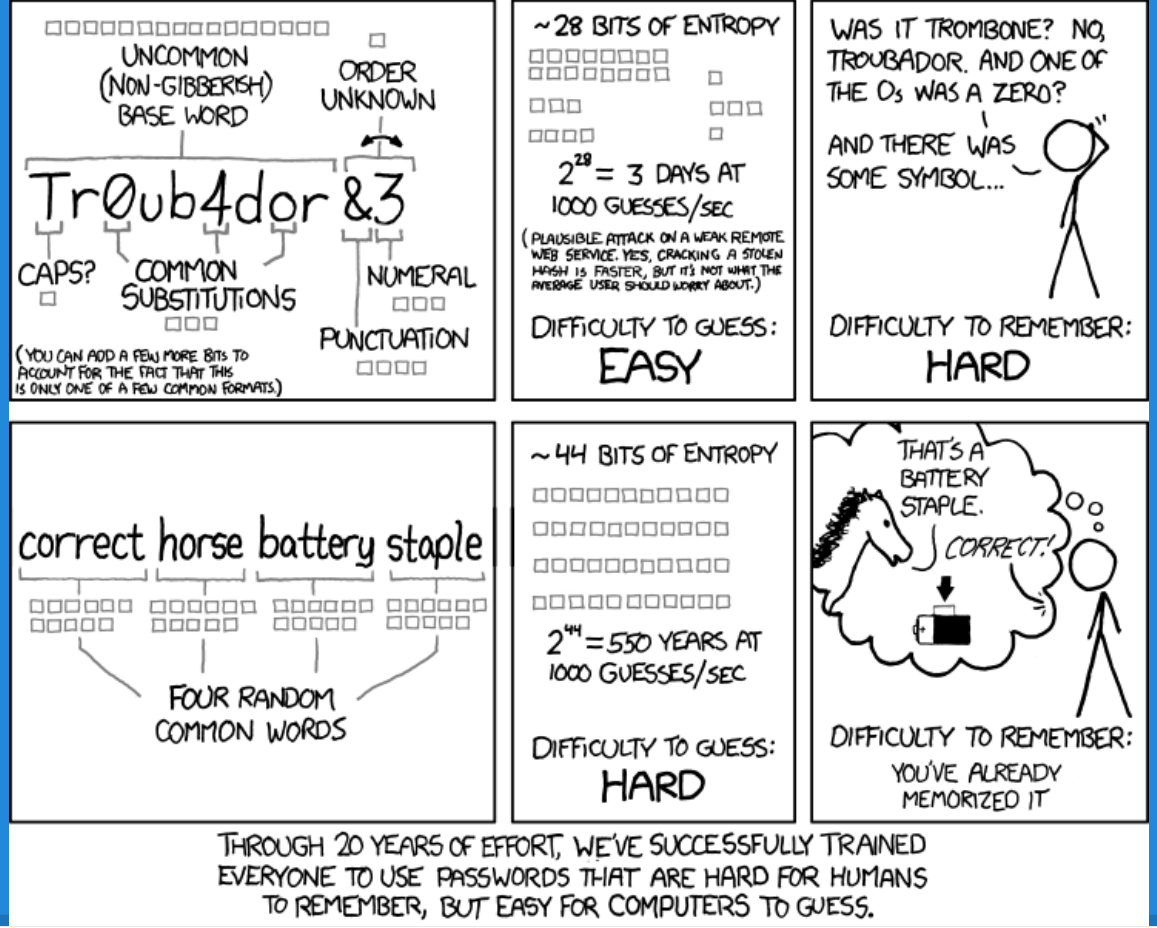
This is a **BIG** security failure.

The Reality,
Top 10 most used Password

1. *123456*
2. *password*
3. *12345*
4. *12345678*
5. *qwerty*
6. *123456789*
7. *1234*
8. *basebal*
9. *dragon*
10. *football*

According to various leaked password accident on internet, compiled by SplashData, via Gizmodo.

Source : ***http://gizmodo.com/the-25-most-popular-passwords-of-2013-god-help-us-1504852434***



Credit to xkcd.com.

Questions

- Metode Crypto Hash apakah yang menghasilkan password yang paling lama dijebol?
- Apakah password berupa “kata-kata” mampu memberikan keamanan yang setara dengan password acak/*random*?

Dasar Kecepatan CRACK

Pada tahun 2012, Jeremi Gosney, seorang ahli Information Security, merakit komputer yang bertenagakan 25 GPU dan mampu mencoba:

- 180 Miliar MD5/detik
- 71.000 Bcrypt/detik

Source : http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

Kekuatan Password

Adalah butuh berapa kali percobaan (asumsi worst case) untuk menemukan password yang benar.

$$\text{Pass strength} = \text{char space}^{\text{length}}$$

Source : https://math.stackexchange.com/questions/1229789/formula-to-calculate-password-cracking-time-in-years-taking-into-account-moore

Waktu untuk *Menjebol* Password

Adalah waktu yang dibutuhkan untuk menemukan password yang sesuai.

Waktu Crack =

Password strength / Kecepatan crack

Source : https://math.stackexchange.com/questions/1229789/formula-to-calculate-password-cracking-time-in-years-taking-into-account-moore

Let’s Introduce Moore Law

Asumsi menyederhanakan:

“Tiap 2 tahun sekali, kecepatan processor naik 2 kali lipat”

Sehingga kecepatan percobaan password diasumsikan **meningkat 2 kali lipat.**

$$f(x) = 2^{(t-t_0)/2}$$

Source : https://math.stackexchange.com/questions/1229789/formula-to-calculate-password-cracking-time-in-years-taking-into-account-moore

METODOLOGI

Variabel Bebas :

waktu (tahun) : berdasarkan hukum moore

Variabel Terikat :

waktu cracking password

Password vs other password

Human password:

`bergelutpanassemesterkacang`

- Random words from KBBI.
- KBBI memiliki ± 92.000 kata.

VS

Random password:

`&oBYILnTra`

- Random words from keyboard.
- Keyboard standard US memiliki 95 karakter.

Pass strength = 92000^4

~= `7.2 * 10^19 kombinasi`

Pass strength = 95^10

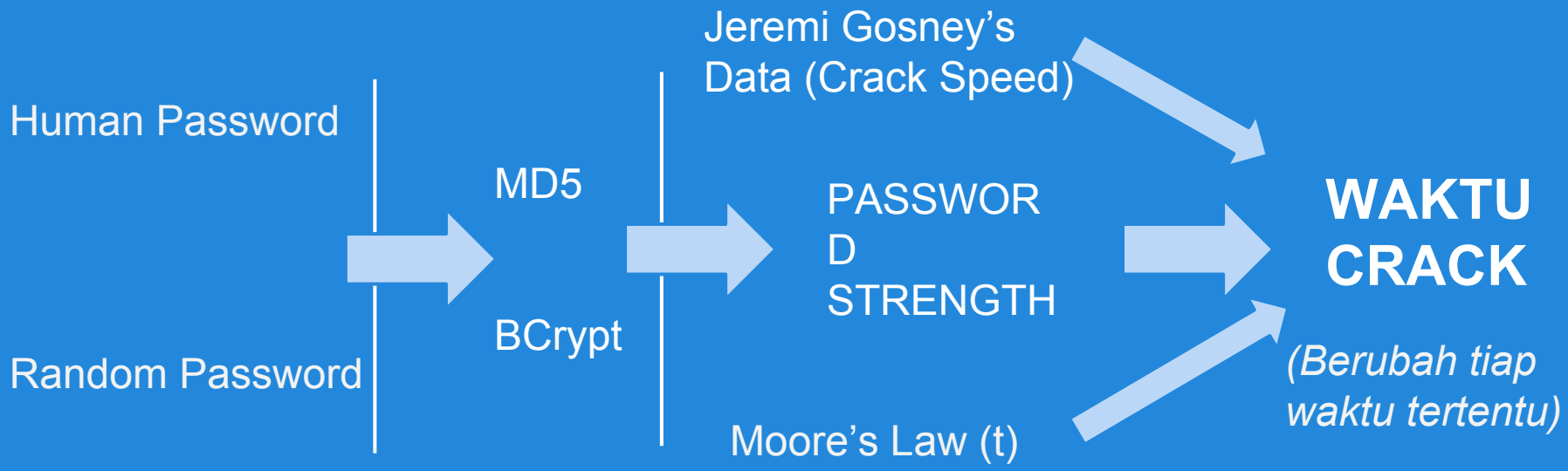
~= `6.0 * 10^19 kombinasi`

Crypto Hash Method

2 (Dua) metode hash yang dibandingkan :

- **MD5 :** sangat umum digunakan di berbagai sistem saat ini.
- **Bcrypt :** metode hash baru yang sedang naik daun. Fitur utamanya adalah algoritmanya **lambat**.

METODOLOGI


Human Password
Random Password
MD5
BCrypt
Jeremi Gosney's
Data (Crack Speed)
PASSWOR
D
STRENGTH
Moore's Law (t)
WAKTU
CRACK
(Berubah tiap
waktu tertentu)

Lama Waktu Cracking Tahun 2012

MD5:

`bergelutpanassemesterkacang:`

Waktu = password strength / kecepatan crack
= 7.2 * 10^19 / 180 * 10^9
= 4 * 10^8 detik
= 12.7 Tahun

`&oBYILnTra :`

Waktu = password strength / kecepatan crack
= 6 * 10^19 / 180 * 10^9
= 3.33 * 10^8 detik
= 10.6 Tahun

Bcrypt:

`bergelutpanassemesterkacang:`

Waktu = password strength / kecepatan crack
= 7.2 * 10^19 / 71000
= 1.0140845 * 10^15 detik
= 32 Juta Tahun

`&oBYILnTra :`

Waktu = password strength / kecepatan crack
= 6 * 10^19 / 71000
= 8.4507042 * 10^14 detik
= 26 Juta Tahun

Lama Waktu Cracking Tahun 2014

MD5:

`bergelutpanassemesterkacang:`

Waktu = password strength / kecepatan crack
= 7.2 * 10^19 / 180 * 10^9 * 2
= 2 * 10^8 detik
= 6.3 Tahun

`&oBYILnTra :`

Waktu = password strength / kecepatan crack
= 6 * 10^19 / 180 * 10^9 * 2
= 1.665 * 10^8 detik
= 5.3 Tahun

Bcrypt:

`bergelutpanassemesterkacang:`

Waktu = password strength / kecepatan crack
= 7.2 * 10^19 / 71000 * 2
= 5.0704225 * 10^14 detik
= 16 Juta Tahun

`&oBYILnTra :`

Waktu = password strength / kecepatan crack
= 6 * 10^19 / 71000 * 2
= 4.2253521 * 10^14 detik
= 13 Juta Tahun

Coding Section (IMPLEMENTATION)

Menggunakan **Python**

Distribusi Anaconda, yaitu Python yang sudah dikemas dengan library scientific lengkap.

(Numpy: manipulasi matrix, Matplotlib: plotting fungsi)

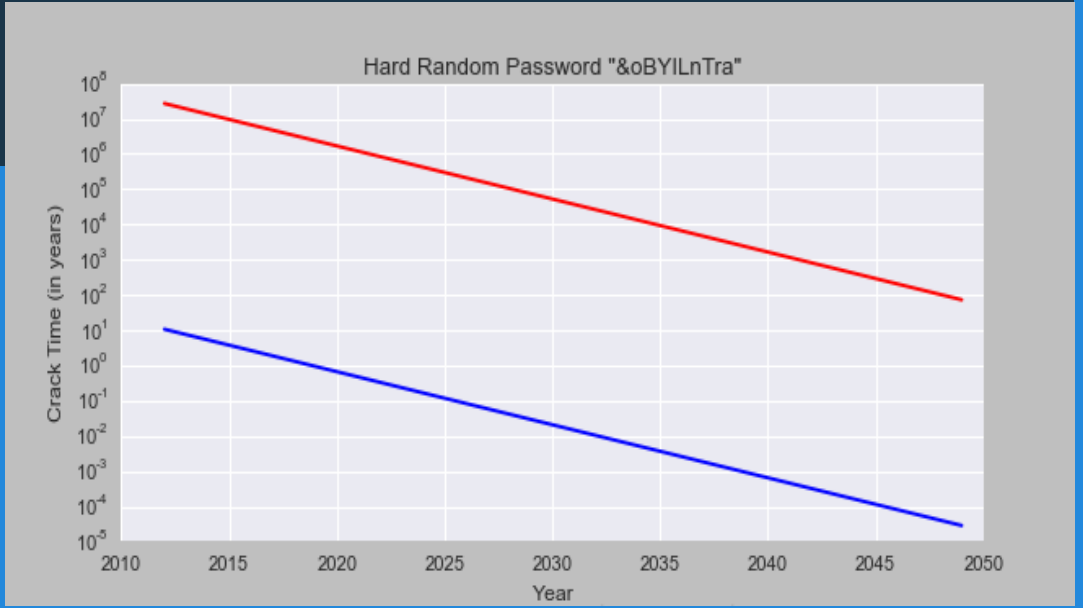
http://continuum.io

```python
import matplotlib.pyplot as plt
import seaborn as sns
import math

# CONSTANT
CURRENT_MD5_CRACK_SPEED    = 180*10**9
CURRENT_SHA1_CRACK_SPEED   = 63*10**9
CURRENT_BCRYPT_CRACK_SPEED = 71000
LOG_OF_2                   = math.log(2)
KBBI_WORD_COUNT            = 92000
STANDARD_US_KEYBOARD_CHAR_COUNT = 95

# SIMULATION CONFIGURATION
START_SIMULATION_YEAR = 2012
END_SIMULATION_YEAR   = 2050
```

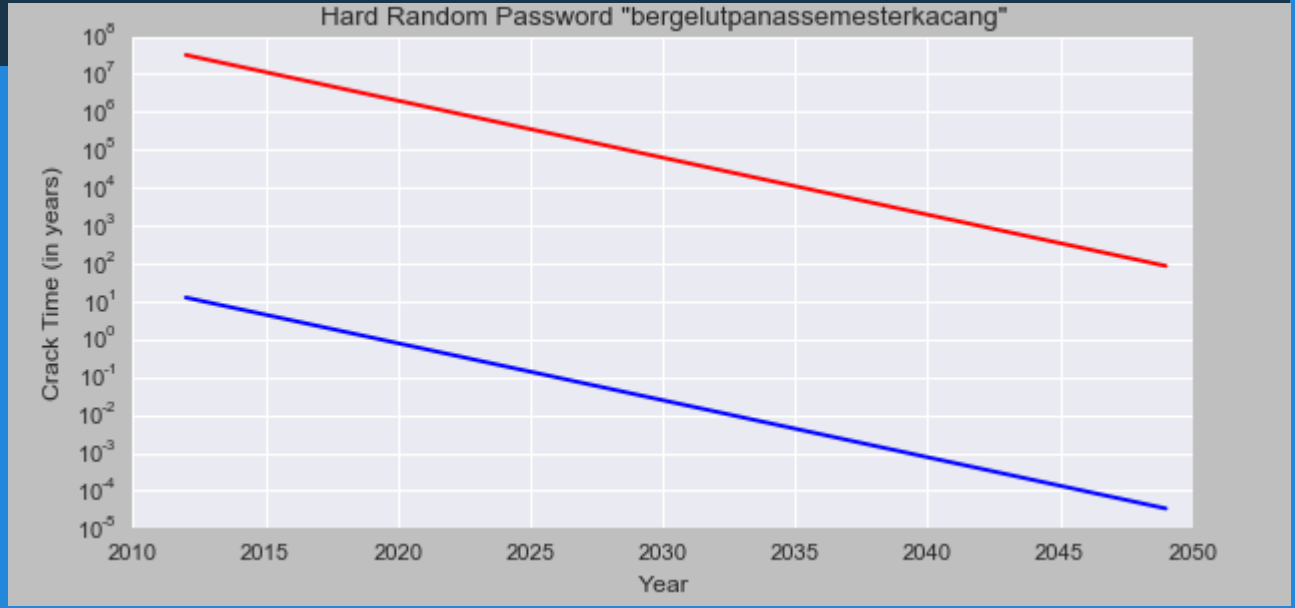
```python
class HashMethod():
    def __init__(self, hashSpeed):
        self.hashSpeed = hashSpeed

    def diffYear(self, currentYear):
        return (currentYear - START_SIMULATION_YEAR)

    def getHashSpeedNow(self, currentYear):
        return self.hashSpeed * math.pow(2, self.diffYear(currentYear)/2)

    def getCrackTime(self, currentYear, password):
        return (password.passwordStrength) / (self.getHashSpeedNow(currentYear)*3600*24*365)
```

```
hard_random_password = Password('&oBYILnTra', 10, STANDARD_US_KEYBOARD_CHAR_COUNT)
hard_human_password  = Password('bergelutpanassemesterkacang', 4, KBBI_WORD_COUNT)
```

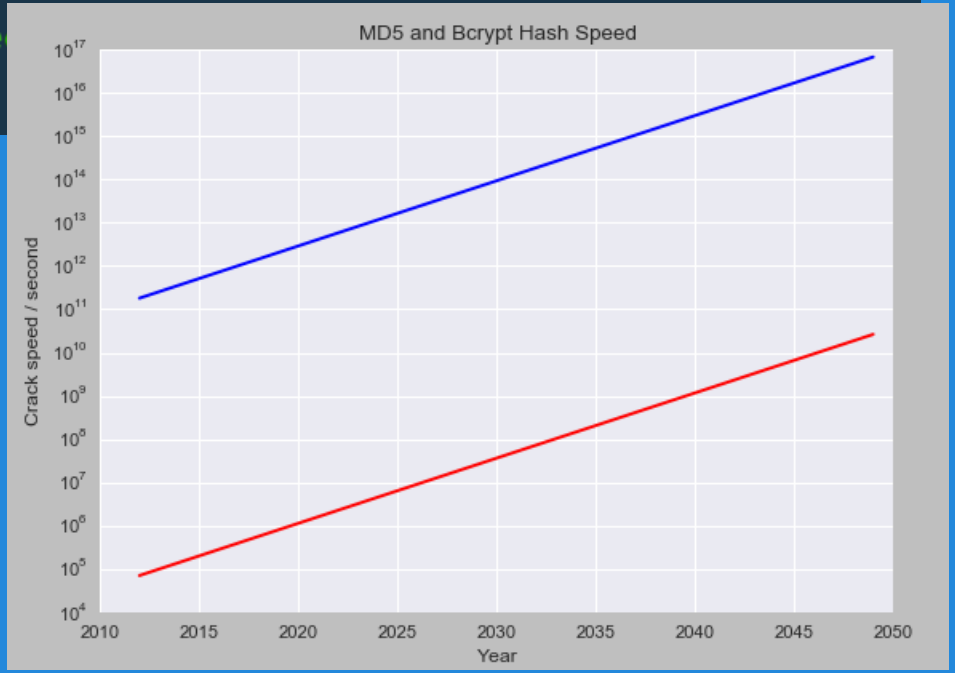
```
# Figure 1: Cracking Time for our password
# Subplot 1 for hard_random_password
plt.figure(1)
plt.subplot(211)
plt.title('Hard Random Password \"&oBYILnTra\"')
plt.plot(years, [MD5.getCrackTime(year, hard_random_password) for year in years], 'b-',
    years, [Bcrypt.getCrackTime(year, hard_random_password) for year in years], 'r-')
plt.yscale('log')
plt.ylabel('Crack Time (in years)')
plt.xlabel('Year')
```

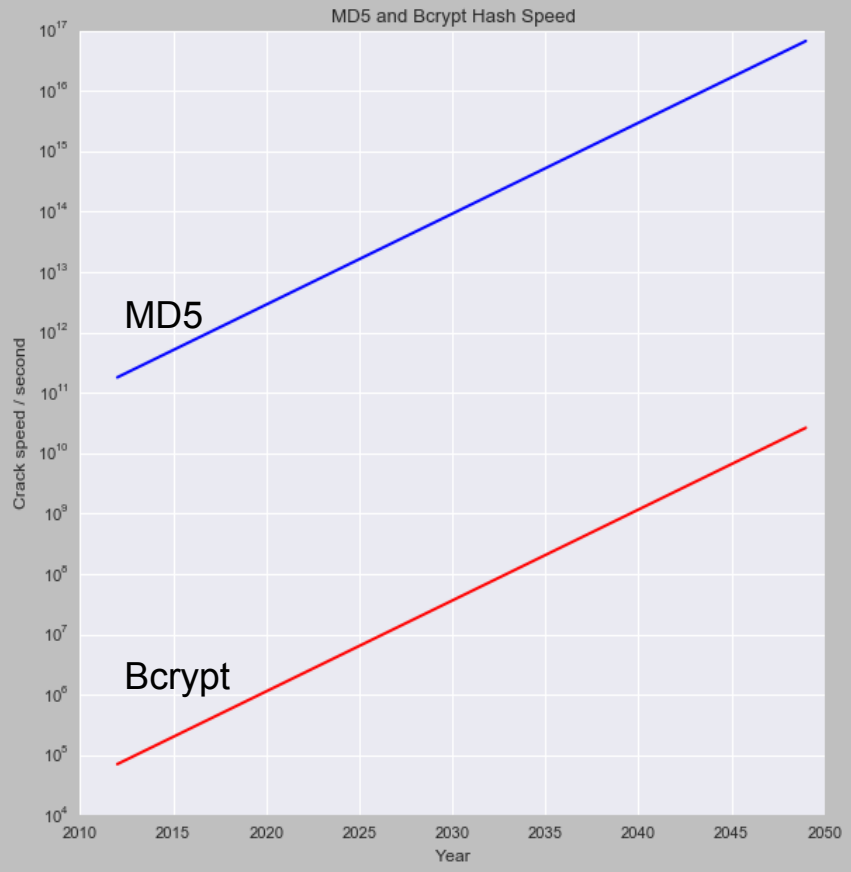


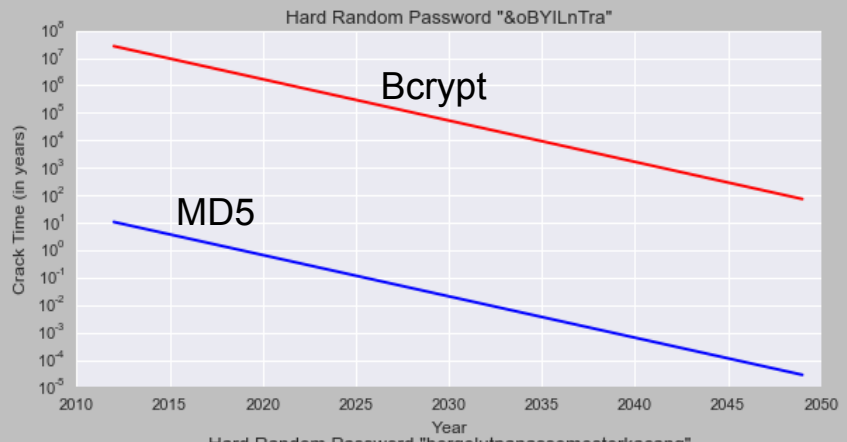
```
# Subplot 2 for hard_human_password
plt.subplot(212)
plt.title('Hard Random Password \"bergelutpanassemesterkacang\"')
plt.plot(years, [MD5.getCrackTime(year, hard_human_password) for year in years], 'b-',
    years, [Bcrypt.getCrackTime(year, hard_human_password) for year in years], 'r-')
plt.yscale('log')
plt.ylabel('Crack Time (in years)')
plt.xlabel('Year')
```

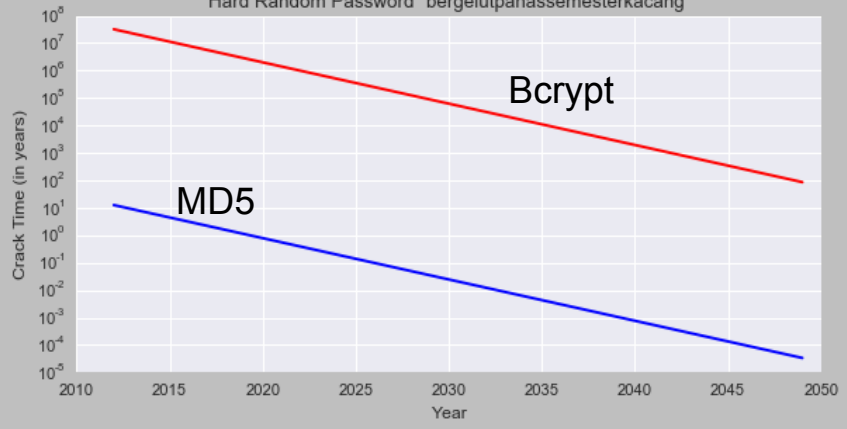


```
# Figure 2: MD5 and Bcrypt Hash Speed
plt.figure(2)
plt.title('MD5 and Bcrypt Hash Speed')
plt.plot(years, [MD5.getHashSpeedNow(year) for year in years], 'b-',
    years, [Bcrypt.getHashSpeedNow(year) for year in years], 'r-')
plt.yscale('log')
plt.ylabel('Crack speed / se
plt.xlabel('Year')
```




MD5 and Bcrypt Hash Speed
Crack speed / second
Year
MD5
Bcrypt


Hard Random Password "&oBYlLnTra"
Crack Time (in years)
Year
Bcrypt
MD5


Hard Random Password "bergelutpanassemesterkacang"
Crack Time (in years)
Year
Bcrypt
MD5

Conclusion

- Bcrypt lebih lambat di*crack* daripada MD5.
- Password dapat dibuat simpel namun tetap kuat.

Sekian dan Terima kasih

Coret2an

1. Jelaskan Background permasalahan kita (Background) slide 3-10, silahkan diringkas,
2. Apa yang mau kita buktikan? (Pertanyaan kita)
3. Bagaimana dasar kita menghitung? (Literature Review)
4. Apa contoh kasus kita? (Method)
5. Bagiamana perhitungan kita? Agak mirip hitung manual aja (Method)
6. Bagaimana kita mensimulasikannya? (Implementation)
7. Bagaimana hasilnya? Apa artinya? (Analysis)
8. Kesimpulan (Summary)

Ternyata modsim batal, hapus aja ni presentasinya