De la cryptographie

Tanguy Ortolo

Debian

21 mai 2012

Table des matières

Vocabulaire

- Chiffrer, déchiffrer, décrypter
- ¬ Crypter, encrypter

Vocabulaire

- Chiffrer, déchiffrer, décrypter
- $\neg$ Crypter, encrypter

Codage

- Chaînes de caractères ⟶ nombres
- Exemples

	A	B	a	é	€
Alphabétique	1	2	–	–	–
Morse	01	1000	–	–	–
ASCII	0x41	0x42	0x61	–	–
Latin-1	0x41	0x42	0x61	0xE9	–
UTF-8	0x41	0x42	0x61	0xC3A9	0xE282AC

Notions
Histoire
Crypto asymétrique
Certification
TLS/SSL
OpenPGP

Codage

- Chaînes de caractères $\longrightarrow$ nombres
- Exemples

	A	B	a	é	€
Alphabétique	1	2	–	–	–
Morse	01	1000	–	–	–
ASCII	0x41	0x42	0x61	–	–
Latin-1	0x41	0x42	0x61	0xE9	–
UTF-8	0x41	0x42	0x61	0xC3A9	0xE282AC

Hachage cryptographique

Message	$\longrightarrow$	condensé de vérification
▶ Toto		998db284485ec6c227f8dc34086128e1
toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \Longrightarrow$ hachages $\neq$
- Hachages $\neq \Longrightarrow$ messages $\neq$

Hachage cryptographique

	Message	$\longrightarrow$	condensé de vérification
▶	Toto		998db284485ec6c227f8dc34086128e1
	toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \implies$ hachages $\neq$
- Hachages $\neq \implies$ messages $\neq$
- Preuve par 9, clef RIB…

Hachage cryptographique

	Message	$\longrightarrow$	condensé de vérification
▶	Toto		998db284485ec6c227f8dc34086128e1
	toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \implies$ hachages $\neq$
- Hachages $\neq \implies$ messages $\neq$
- Preuve par 9, clef RIB...

Hachage cryptographique

Message	$\longrightarrow$	condensé de vérification
Toto		998db284485ec6c227f8dc34086128e1
toto		f71dbe52628a3f83a77ab494817525c6
- Messages $\neq \Longrightarrow$ hachages $\neq$
- Hachages $\neq \Longrightarrow$ messages $\neq$
- Preuve par 9, clef RIB…

Hachage cryptographique

Message	$\longrightarrow$	condensé de vérification
Toto		998db284485ec6c227f8dc34086128e1
toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \Longrightarrow$ hachages $\neq$
- Hachages $\neq \Longrightarrow$ messages $\neq$
- Preuve par 9, clef RIB...

Hachage cryptographique

	Message	$\longrightarrow$	condensé de vérification
▶	Toto		998db284485ec6c227f8dc34086128e1
	toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \Longrightarrow$ hachages $\neq$
- Hachages $\neq \Longrightarrow$ messages $\neq$
- Preuve par 9, clef RIB…

Hachage cryptographique

	Message	$\longrightarrow$	condensé de vérification
▶	Toto		998db284485ec6c227f8dc34086128e1
	toto		f71dbe52628a3f83a77ab494817525c6

- Messages $\neq \implies$ hachages $\neq$
- Hachages $\neq \implies$ messages $\neq$
- Preuve par 9, clef RIB...

Chiffres historiques

Stéganographie

César
```
  IL FAIT BEAU
+ 33 3333 3333
= LO IDLW EHDX
```

Autres mono-alphabétiques

Attaques fréquence des lettres

Chiffres historiques

Stéganographie

César

```
  IL FAIT BEAU
+ 33 3333 3333
= LO IDLW EHDX
```

Autres mono-alphabétiques

Attaques fréquence des lettres

Chiffres historiques

Stéganographie

César	`IL FAIT BEAU`
	`+ 33 3333 3333`
	`= LO IDLW EHDX`
Autres	mono-alphabétiques
Attaques	fréquence des lettres

Course au chiffre

- Chiffres manuels

  1586 Vigenère

  ```
  IL FAIT BEAU
  CL EFCL EFCL
  LX KGLF GKDG
  ```

  1854 Attaque de Babbage

- Chiffres mécaniques

  1919–1926 Enigma

  1933–1941 Attaque complexe...

- Chiffres électroniques : DES, 3DES, AES...

Course au chiffre

- Chiffres manuels

  1586 Vigenère

  ```
  IL FAIT BEAU
  CL EFCL EFCL
  LX KGLF GKDG
  ```

  1854 Attaque de Babbage

- Chiffres mécaniques

  1919–1926 Enigma

  1933–1941 Attaque complexe...

- Chiffres électroniques : DES, 3DES, AES...

Course au chiffre

- Chiffres manuels

  1586 Vigenère

  ```
  IL FAIT BEAU
  CL EFCL EFCL
  LX KGLF GKDG
  ```

  1854 Attaque de Babbage

- Chiffres mécaniques

  1919–1926 Enigma

  1933–1941 Attaque complexe...

- Chiffres électroniques : DES, 3DES, AES...

Cryptographie asymétriques

- Chiffres symétriques : secret partagé...
- Échange de clefs

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ g & \longleftrightarrow & g \\ a & \xrightarrow{g^a} & g^a \\ g^b & \xleftarrow{g^b} & b \\ g^{ab} & & g^{ab} \end{array}$$

- Chiffres asymétriques

Cryptographie asymétriques

- Chiffres symétriques : secret partagé...
- Échange de clefs
$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ g & \longleftrightarrow & g \\ a & \xrightarrow{g^a} & g^a \\ g^b & \xleftarrow{g^b} & b \\ g^{ab} & & g^{ab} \end{array}$$
- Chiffres asymétriques

Cryptographie asymétriques

- Chiffres symétriques : secret partagé...
- Échange de clefs

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ g & \longleftrightarrow & g \\ a & \xrightarrow{g^a} & g^a \\ g^b & \xleftarrow{g^b} & b \\ g^{ab} & & g^{ab} \end{array}$$

- Chiffres asymétriques

Principes généraux

- Fonctions à sens unique avec trappe :
  - f_P
  - f_P^{-1} ??
  - $f_S = f_P^{-1}$!
- $P =$ clef publique
- $S =$ clef privée – secrète
- Inconvénient : lent...

Principes généraux

- Fonctions à sens unique avec trappe :
  - f_P
  - f_P^{-1} ??
  - $f_S = f_P^{-1}$!
- P = clef publique
- S = clef privée – secrète
- Inconvénient : lent...

Principes généraux

- Fonctions à sens unique avec trappe :
  - f_P
  - f_P^{-1} ??
  - $f_S = f_P^{-1}$!
- P = clef publique
- S = clef privée – secrète
- Inconvénient : lent...

Utilisation pratique

	Alice		Bob
Transmission			
	(A, A')	$\xrightarrow{A}$	A
	B	$\xleftarrow{B}$	(B, B')
Chiffrement	M		
	$M' = f_B(M)$	$\xrightarrow{M'}$	M'
			$M = f_{B'}(M')$
Signature	M		
	$M^* = f_{A'}(M)$	$\xrightarrow{M^*}$	M^*
			$f_A(M^*) \stackrel{?}{=} M$

Utilisation pratique

Transmission	Alice		Bob
	(A, A')	$\xrightarrow{A}$	A
	B	$\xleftarrow{B}$	(B, B')
Chiffrement	M		
	$M' = f_B(M)$	$\xrightarrow{M'}$	M'
			$M = f_{B'}(M')$
Signature	M		
	$M^* = f_{A'}(M)$	$\xrightarrow{M^*}$	M^*
			$f_A(M^*) \stackrel{?}{=} M$

Utilisation pratique

	Alice		Bob
Transmission	(A, A')	$\xrightarrow{A}$	A
	B	$\xleftarrow{B}$	(B, B')
Chiffrement	M		
	$M' = f_B(M)$	$\xrightarrow{M'}$	M'
			$M = f_{B'}(M')$
Signature	M		
	$M^* = f_{A'}(M)$	$\xrightarrow{M^*}$	M^*
			$f_A(M^*) \stackrel{?}{=} M$

Problème de l'authenticité des clefs

- Problème : vraie clef d'Alice ?
- Attaque de *l'homme du milieu*

Alice		Oscar		Bob
(A, A')	$\xrightarrow{A}$	(O, O')	$\xrightarrow{O}$	
M	$\xleftarrow{f_A(M)}$	M	$\xleftarrow{f_O(M)}$	M

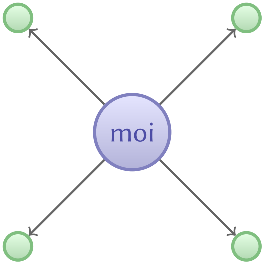
Problème de l'authenticité des clefs

- Problème : vraie clef d'Alice ?
- Attaque de *l'homme du milieu*

Alice		Oscar		Bob
(A, A')	$\xrightarrow{A}$	(O, O')	$\xrightarrow{O}$	
M	$\xleftarrow{f_A(M)}$	M	$\xleftarrow{f_O(M)}$	M

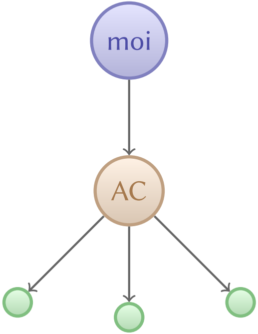
Confiance directe

- Transmission en personne
- Inconvénient : peu efficace



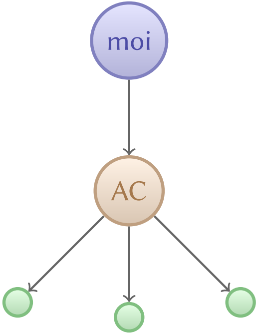
Autorités de certification

- Déléguer sa confiance
- Autorité de certification : reconnue par « les gens »
- Certificat :
  - Clef publique, identité
  - Signature d'une autorité
- Utilisé pour SSL sur Internet
- Avantage : répond au problème
- Inconvénients :
  - pas de contrôle citoyen
  - peu nombreuses
  - vérifient mal
  - pas forcément intègres



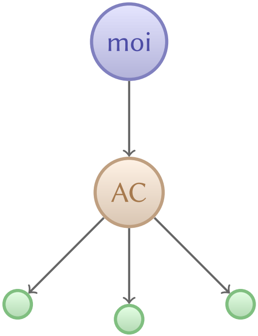
Autorités de certification

- Déléguer sa confiance
- Autorité de certification : reconnue par « les gens »
- Certificat :
  - Clef publique, identité
  - Signature d'une autorité
- Utilisé pour SSL sur Internet
- Avantage : répond au problème
- Inconvénients :
  - pas de contrôle citoyen
  - peu nombreuses
  - vérifient mal
  - pas forcément intègres



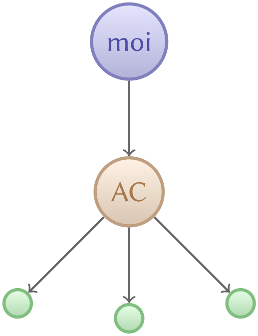
Autorités de certification

- Déléguer sa confiance
- Autorité de certification : reconnue par « les gens »
- Certificat :
  - Clef publique, identité
  - Signature d'une autorité
- Utilisé pour SSL sur Internet
- Avantage : répond au problème
- Inconvénients :
  - pas de contrôle citoyen
  - peu nombreuses
  - vérifient mal
  - pas forcément intègres



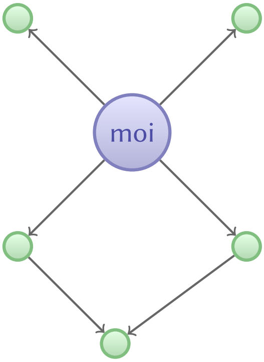
Autorités de certification

- Déléguer sa confiance
- Autorité de certification : reconnue par « les gens »
- Certificat :
  - Clef publique, identité
  - Signature d'une autorité
- Utilisé pour SSL sur Internet
- Avantage : répond au problème
- Inconvénients :
  - pas de contrôle citoyen
  - peu nombreuses
  - vérifient mal
  - pas forcément intègres



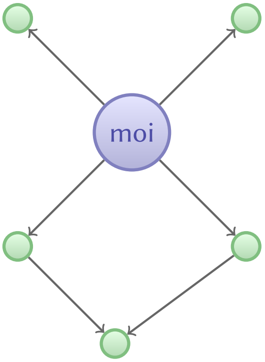
Réseau de confiance

- Certifications multiples
- Autorités de certifications : potentiellement tout le monde
- Certificat :
  - Clef publique, identité
  - Signature d'un garant n°1
  - Signature d'un garant n°2
  - ...
- Avantage : *beaucoup* plus résistant
- Inconvénients :
  - lent à construire
  - aucun intérêt commercial



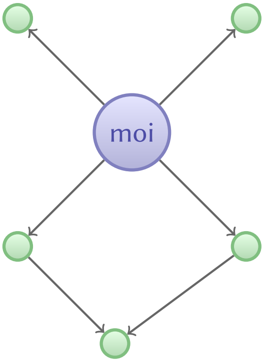
Réseau de confiance

- Certifications multiples
- Autorités de certifications : potentiellement tout le monde
- Certificat :
  - Clef publique, identité
  - Signature d'un garant n°1
  - Signature d'un garant n°2
  - ...
- Avantage : *beaucoup* plus résistant
- Inconvénients :
  - lent à construire
  - aucun intérêt commercial



Réseau de confiance

- Certifications multiples
- Autorités de certifications : potentiellement tout le monde
- Certificat :
  - Clef publique, identité
  - Signature d'un garant n°1
  - Signature d'un garant n°2
  - ...
- Avantage : *beaucoup* plus résistant
- Inconvénients :
  - lent à construire
  - aucun intérêt commercial



Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :

Clef privée

- Clef publique

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas

Clef privée

Demande

- Clef publique
- Nom de domaine

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas
  3. clef de chiffrement symétrique

     flux chiffré

Clef privée

Certificat
▶ Clef publique ▶ Nom de domaine ▶ Signature

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas
  3. clef de chiffrement symétrique
  4. flux chiffré

Clef privée

Certificat
Clef publique
Nom de domaine
Signature

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas
  3. clef de chiffrement symétrique
  4. flux chiffré

Clef privée

Certificat
- Clef publique
- Nom de domaine
- Signature

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas
  3. clef de chiffrement symétrique
  4. flux chiffré

Clef privée

Certificat
▶ Clef publique ▶ Nom de domaine ▶ Signature

Transport layer security

- Serveur :
  1. paire de clefs
  2. demande de certificat
  3. certification
- Client :
  - liste d'autorités
- Connexion à un serveur :
  1. serveur : certificat
  2. client : accepte ou pas
  3. clef de chiffrement symétrique
  4. flux chiffré

Clef privée

Certificat
- Clef publique
- Nom de domaine
- Signature

Cas pratiques

- 

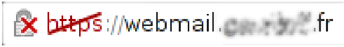
  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
- 

  - transmission chiffrée
  - propriétaire de la clef garanti

Cas pratiques

- 

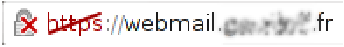
  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
  - invulnérable : écoutes simples
  - vulnérable : interceptions
- 

  - transmission chiffrée
  - propriétaire de la clef garanti

Cas pratiques

- 

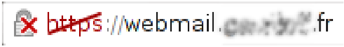
  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
  - invulnérable : écoutes simples
  - vulnérable : interceptions
- 

  - transmission chiffrée
  - propriétaire de la clef garanti

Cas pratiques

- 

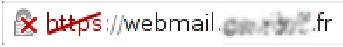
  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
  - invulnérable : écoutes simples
  - vulnérable : interceptions
- 

  - transmission chiffrée
  - propriétaire de la clef garanti
  - invulnérable : écoutes, interceptions
  - vulnérable : vol de clef, corruption d'une AC

Cas pratiques

- 

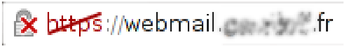
  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
  - invulnérable : écoutes simples
  - vulnérable : interceptions
- 

  - transmission chiffrée
  - propriétaire de la clef garanti
  - invulnérable : écoutes, interceptions
  - vulnérable : vol de clef, corruption d'une AC

Cas pratiques

- 

  - transmission en clair
  - vulnérable : écoutes, interceptions
  - données sensibles : fuyez !
- 

  - transmission chiffrée
  - propriétaire de la clef ?
  - invulnérable : écoutes simples
  - vulnérable : interceptions
- 

  - transmission chiffrée
  - propriétaire de la clef garanti
  - invulnérable : écoutes, interceptions
  - vulnérable : vol de clef, corruption d'une AC

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Origine

- Zimmermann
  - vie privée menacée
  - cryptographie
  - restrictions
  - développer tant que c'est possible
  - succès indirect
- Pretty good privacy — PGP
  - cryptographie asymétrique
  - réseau de confiance
  - semi-libre, livre imprimé
- OpenPGP : normalisation
- GnuPG — GPG : mise en œuvre libre

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

- Clef privée

- Clef publique
- Photo

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

- Clef privée

- Clef publique
- Photo

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

4B10 D847

- Clef privée

4B10 D847

- Clef publique
- Photo

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

4B10 D847

- Clef privée

4B10 D847

- Clef publique
- Prénom Nom <adr1>
- Prénom Nom <adr2>
- Photo

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

4B10 D847

- Clef privée

4B10 D847

- Clef publique
- Prénom Nom <adr1>
  - Auto-signature
  - Signature de Untel
- Prénom Nom <adr2>
  - Auto-signature
- Photo

Notions

- Clef
  - privée, publique
  - empreinte
  - identifiant
- Identités
- Signatures
- Modèle de confiance

4B10 D847
▶ Clef privée

4B10 D847
▶ Clef publique
▶ Prénom Nom <adr1>
▶ Auto-signature
▶ Signature de Untel
▶ Prénom Nom <adr2>
▶ Auto-signature
▶ Photo