

Sécurité des Transactions

Protection de l'information

Bases mathématiques pour la sécurité informatique

Première partie Principes de base



Jean-Luc Stehlé
EPITA FMSI ING 1
30 Avril 2014

Jean-Luc.Stehle@NormaleSup.org

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 1

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Planning des cours

Date	Code Cours	Horaire	Nb heures	Lieu	Promo	Cursus	Activité	Enseignant	N° de Salle	SEM	Intitulé du cours
mercredi 30 avril 2014	FMSI	09h00 à 12h00	3,0	KREMLIN	2016	ING1	COURS	STEHLE.Jean-Luc	amphi 3	S2	Fondements mathématiques pour la sécurité informatique
mercredi 14 mai 2014	FMSI	09h00 à 12h00	3,0	KREMLIN	2016	ING1	COURS	STEHLE.Jean-Luc	amphi 3	S2	Fondements mathématiques pour la sécurité informatique
mercredi 21 mai 2014	FMSI	09h00 à 12h00	3,0	KREMLIN	2016	ING1	COURS	STEHLE.Jean-Luc	amphi 3	S2	Fondements mathématiques pour la sécurité informatique
mercredi 28 mai 2014	FMSI	09h00 à 12h00	3,0	KREMLIN	2016	ING1	COURS	STEHLE.Jean-Luc	amphi 3	S2	Fondements mathématiques pour la sécurité informatique

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 2

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Bases mathématiques pour la sécurité de l'information

- Sensibilisation générale
- Protocoles classiques (Diffie Helmann, RSA...)
- Compléments d'arithmétique modulaire
- Bases mathématiques pour l'AES
- Courbes elliptiques

Jean-Luc.Stehle@NormaleSup.org

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 3



BIBLIOGRAPHIE

- **B. Beckett** Introduction aux méthodes de la cryptologie *Masson 1990*
- **G. Brassard** Cryptologie contemporaine *Masson 1993*
- **G. Konheim** Cryptography : A primer *John Wiley 1981*
- **E. Kranakis** Primality and Cryptography *John Wiley 1986*
- **D.E.R. Denning** Cryptography and data security *Addison Wesley 1983*
- **X. Marsault** **Compression et cryptage en informatique** *Hermès Paris 1992*
- **G. Robin** Algorithmique et cryptographie *Ellipses Paris 1991*
- **B. Schneier** **Applied cryptography** *John Wiley 1993*
Cryptologie Appliquée *Thomson Publishing 1997*
- **M.R. Schroeder** Number Theory in Science and Communication
with applications in Cryptography, Physics, Digital Information, Computing,...
Springer 1986
- **J.H. Van Lint** **Introduction to Coding Theory** *Springer 1982*

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 4



BIBLIOGRAPHIE (Suite)

Revue « Pour la Science » *Dossier spécial N° 36* Juillet/Octobre 2002

**Excellente synthèse de l'état de
l'art actuel**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

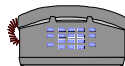
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 5

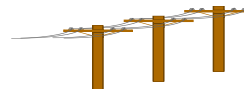


Quelques exemples instructifs

- Distributeurs de billets
- Changeurs de devises
- Piratage du téléphone



- Ralentissement de SWIFT



- Fichiers de malades
- Commerce électronique



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

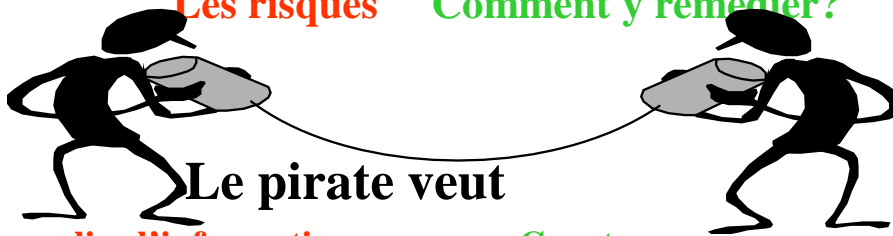
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 6



Sécurité des transactions

Les risques Comment y remédier?



Le pirate veut

- lire l'information Cryptage
- modifier l'information Scellement
- se faire passer pour l'interlocuteur Authentification
Signature électronique

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 7



Sécurité des transactions

Les risques Comment y remédier?

- L'émetteur renie sa parole Non répudiation
- Les deux interlocuteurs sont-ils bien d'accord ?

Problème des accusés de réception...

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 8



Le problème des généraux byzantins



Armée A



Armée B



Armée C

$$A < C$$

$$B < C$$

$$A + B > C$$

**Comment communiquer entre A et B
en assurant le consensus ?**

- Problème de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack de l'Ack.....
- **Problème des « connaissances communes »**

© Aurélien Leteinturier

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 9

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Le Scellement

MESSAGE

Sceau ★

- **Sceau = f(Message, clé de scellement)**
Assure que le message n'a pas été modifié

- **Problème de la non répudiation**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 10

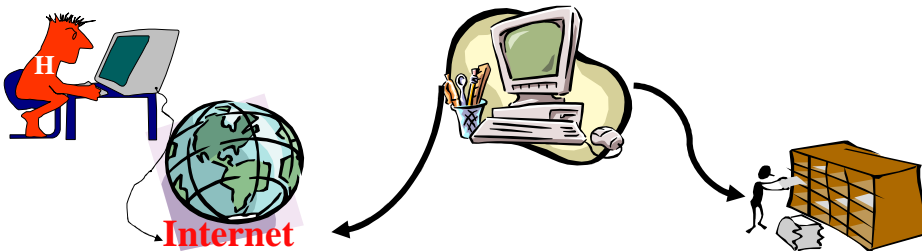
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Divers types d'attaque

- Écoute passive
- Écoute avec partie du clair connu
- Le pirate peut envoyer des messages de son choix
- **Le pirate se fait passer pour l'interlocuteur**



Le problème de la « tête de pont »



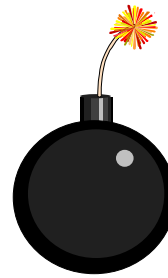
Il faudrait autant de réseaux physiques différents qu'il y a de projets ou d'applications différentes



Divers types d'attaque : le pirate peut injecter



- Un **virus**
- Un **cheval de Troie**
- Une **bombe logique**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

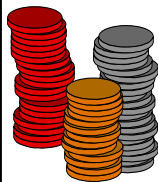
30 Avril 2014, page 13



Principes de base de la protection (1)

**Le pirate dispose de toutes les
ressources de la technique**

- Il est prêt à y mettre le prix
- Chiffrer



- Coût du piratage
- Bénéfice pour le pirate
- Prix à payer pour la protection



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 14



Principes de base de la protection (2)

On est à la merci d'une faille humaine

- **Tout homme a un prix**

Complicités internes

Chantage (*La carotte ou le bâton*)

- **Pourquoi l'employé trahit-il ?**

- pour s'enrichir
- par malveillance, vengeance,...
- par jeu

- **Profil psychologique et socioprofessionnel des employés ayant la possibilité de trahir**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

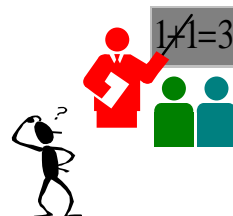
30 Avril 2014, page 15



Principes de base de la protection (3)

On est à la merci des progrès

- **de la technique**
- **des mathématiques**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 16



Principes de base de la protection (4)

Le pirate a de la chance

- S'il y a une faille, il la trouvera
- Rechercher le maillon faible

L'information est-elle piratable avant cryptage ?

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 17

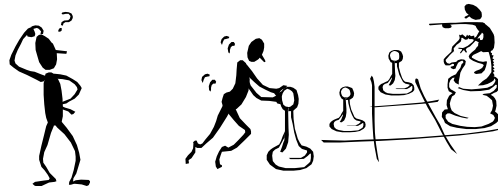


Principes de base de la protection

Approche globale de la sécurité

Jeu d'échec

- Le pirate a les blancs
- Il faut prévoir d'avance sa stratégie



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

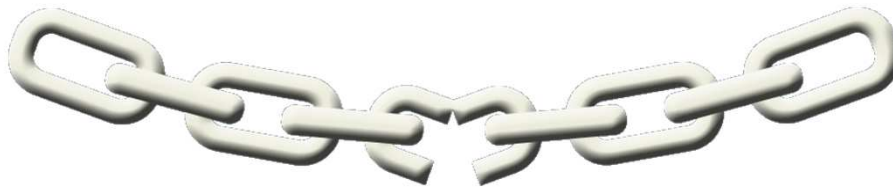
Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 18



Principes de base de la protection



**La solidité d'une chaîne est
celle de son maillon le plus faible**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 19

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les éléments de la sécurité

1. Communication

- **Authentification**

On peut accepter un algorithme lent



- **Partage d'une clé de codage**

doit être modifiée souvent

- **Codage proprement dit**

nécessite un algorithme rapide

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 20

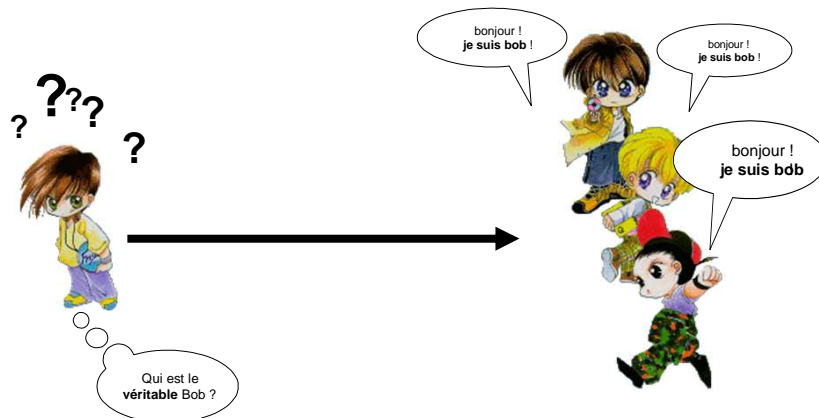
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

2. Contrôle

- **Accusé de réception**
- **Scellement**
- **Non répudiation**

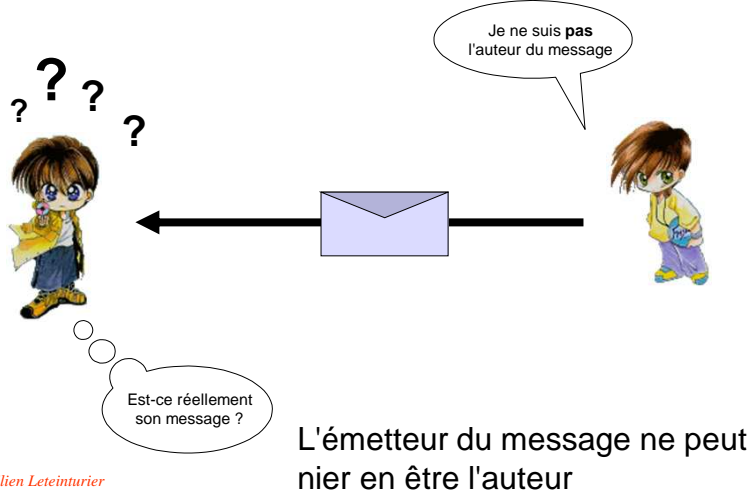


Authentification des interlocuteurs



Être sûr de l'identité de l'interlocuteur

Non répudiation



© Aurélien Leteinturier

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

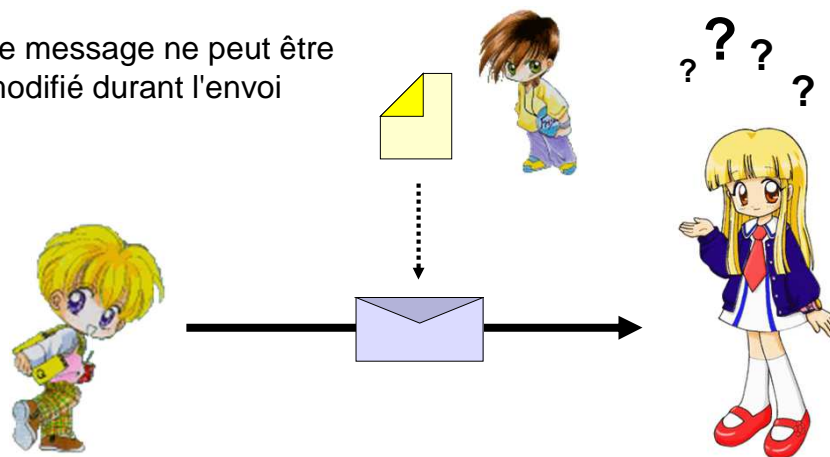
Sécurité des Transactions

30 Avril 2014, page 23

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Sceau / signature

Le message ne peut être modifié durant l'envoi



© Aurélien Leteinturier

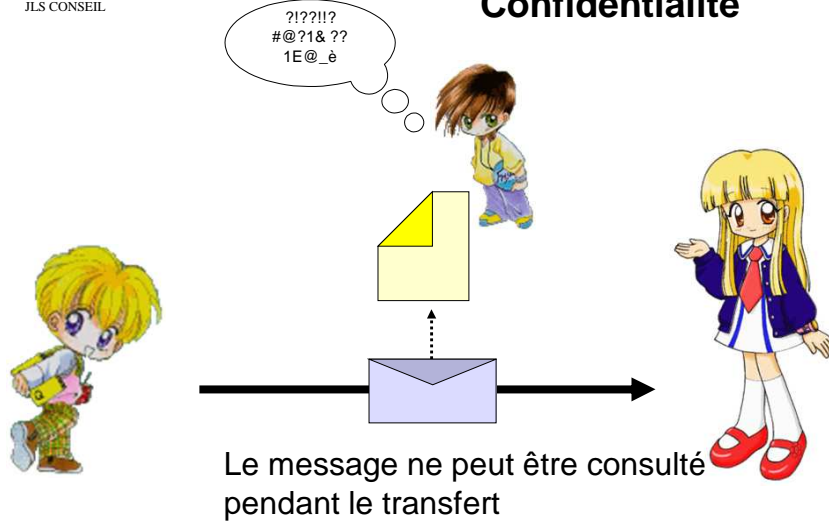
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 24

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Confidentialité



© Aurélien Leteinturier

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 25

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Les éléments de la sécurité

3. Aspects légaux

- **Législations contraignantes**
- **Trouver le juste compromis entre**

- Assurer la sécurité des transmissions «honnêtes»
- Empêcher qu'un système trop sécurisé permette
 - trafics divers...
 - blanchiment d'argent sale
 - Réseaux pédophiles
 - Terrorisme
 - ...



Justice
Liberté
Sécurité

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 26

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Exemples de codes de cryptage

- **Codes historiques**
 - César, Vigenère
 - Masques XOR
 - Multicanaux
- **DES Data Encryption Standard**
 - Blocs de 64 bits
 - Standard USA depuis 1977
 - Algorithme symétrique (même clé de part et d'autre)
- **Méthode du colis à deux cadenas**
- **AES**
- **RSA**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 27

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Code de cryptage

- **Le problème de la backdoor**
 - Un algorithme ne devrait être utilisé qu'après que toute la communauté des cryptographes ne l'ait validé
 - Recherche de failles
 - Recherche de backdoor
- **Et encore...**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 28

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Histoire de la cryptographie : Chiffre de César et dérivés

- On peut rendre le système de César plus robuste par création d'un alphabet mélangé :
 $ABCDEFGHIJKLMNOPQRSTUVWXYZ$
 $MPLOKINJUBHYVGTCTFRXDEWSZQA$

Un tel système fut utilisé à la Renaissance. Il y a dans ce cas $26!$ soit 4.10^{26} clés possibles, la difficulté étant de les retenir :



© Franquin

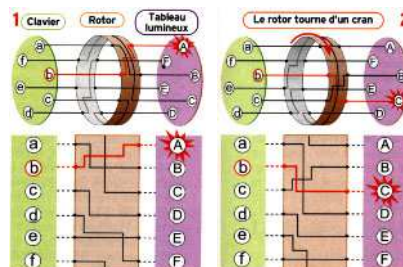
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 29

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Histoire de la cryptographie : La machine Enigma



Le crypt(1)
d'UNIX
fonctionne
encore sur
ce principe

Utilisée par l'Allemagne Nazie : 3 rotors avec alphabet mélangé câblé changé à chaque caractère par rotation des rotors. Equivalent à un masque de période $26 \times 26 \times 26 = 17576$.

Fut cryptanalysée avec succès par les alliés...

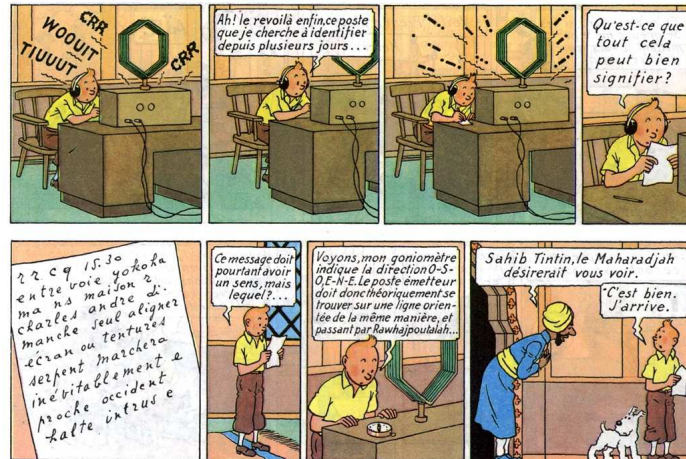
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 30

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Cryptographie vs Stéganographie



© Hergé

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 31

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Stéganographie



Stéganographie (du Grec steganos : couvert) : message caché (par un procédé secret) dans un autre d'apparence anodine

Un cryptogramme n'a pas une apparence anodine, c'est en général un inextricable charabia (gibberish).

© Hergé

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 32

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Un exemple littéraire

d'après G. Sand

Je suis émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une folle envie de me faire danser, je garde le souvenir de votre baiser et je voudrais bien que ce soit la preuve que je puisse être aimée par vous, je suis prête à vous montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler sans nul artifice mon âme toute nue, veuillez me faire une visite. Nous causerons franchement en ami

Je vous prouverai que je suis la femme sincère et capable de vous offrir l'affection la plus profonde comme la plus étroite amitié : en un mot, la meilleure épouse que vous puissiez rêver. Puisque votre âme est libre, pensez que la détresse où j'habite est bien longue, bien dure et souvent bien difficile à vivre et me cause une peine très grosse. Accourez bien vite et venez me la faire oublier. A l'amour, je vais me soumettre.

© George Sand

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 33

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Un exemple de cryptogramme

d'après G. Sand

Je suis émue de vous dire que j'ai bien compris l'autre soir que vous aviez **toujours une folle envie de me faire danser, je garde le souvenir de votre baiser et je voudrais bien que ce soit la preuve que je puisse être aimée par vous, je suis prête à vous montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler sans nul artifice mon âme toute nue, veuillez me faire une visite.** Nous causerons franchement en ami

Je vous prouverai que je suis la femme sincère et capable de vous offrir l'affection **la plus profonde comme la plus étroite amitié : en un mot, la meilleure épouse que vous puissiez rêver. Puisque votre âme est libre, pensez que la détresse où j'habite est bien longue, bien dure et souvent bien difficile à vivre et me cause une peine très grosse. Accourez bien vite et venez me la faire oublier. A l'amour, je vais me soumettre.**

© George Sand

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 34

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les codes asymétriques

RSA : Système asymétrique

A dispose d'une clé publique et d'une clé privée

- **Tout le monde peut envoyer un message confidentiel que seul A peut lire**

Cryptage

- **A peut signer : tout le monde peut vérifier sa signature**

Authentification

- **Semble le meilleur actuellement**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 35



Les codes asymétriques

Inconvénients de RSA

- **Lent**
- **A la merci des progrès de mathématiques**
- **Problème de génération/gestion des clés**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 36

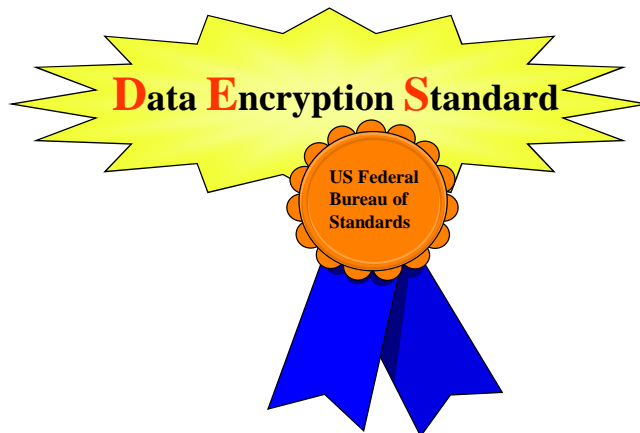
Conclusion



- **Nombreux algorithmes, nombreuses techniques**
- **Difficultés de mise en place**
 - Gestion des clés
 - Failles humaines
- **Sécurité = approche globale**
 - Traquer **toutes** les failles du système
 - Approche globale

Compléments sur le DES

Le « Standard » ancien





DES : Data Encryption Standard

- **1977 US Federal Bureau of Standards**



- *non autorisé pour le secret défense aux USA*

- **Facile à implémenter**
300 lignes Fortran

- **Lent si implémentation logicielle**

- **Rapide si implémentation Hard**
100 Mbits/s en 1993

Algorithme public

- **Blocs de 64 bits (8 octets)**

- **Clés à 56 bits, symétrique**

Seule attaque connue

Essai de toutes les $2^{56} = 7.2 \cdot 10^{16}$ clés
par recherche exhaustive

- **Vulnérabilité**

La gestion des clés
Clés «faibles»



Améliorations

- **Triple DES**

$$c = \text{Des}_{k1}(\text{Des}_{k2}^{-1}(\text{Des}_{k1}(m)))$$

$$m = \text{Des}_{k1}^{-1}(\text{Des}_{k2}(\text{Des}_{k1}^{-1}(c)))$$

- **Mode CBC**

Cipher Block Chaining

$$m = m_1 m_2 m_3 \dots m_n \dots$$

$$c_i = \text{Des}_k(m_i \oplus c_{i-1})$$

$$m_i = c_{i-1} \oplus \text{Des}_k^{-1}(c_i)$$

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 39

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

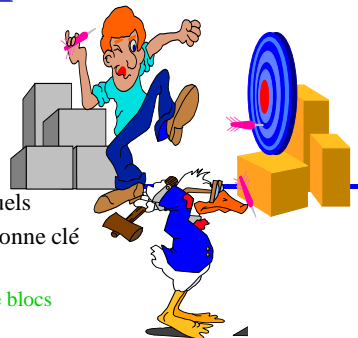


DES : Data Encryption Standard

- **Casser le DES ?**

- **Recherche exhaustive**

- $2^{56} = 72 \times 10^{15}$ clés à tester
- A la portée des moyens de calcul actuels
- Comment savoir qu'on a trouvé la bonne clé
 - Attaque à clair connu
 - D'autant plus facile qu'on a plus de blocs



- **Attaques sans cassage de code**

- **Blocs rejoués**

- **Ajouter un MAC ?**

Banque émetteur	15 blocs
Banque bénéficiaire	15 blocs
Nom déposant	6 blocs
Numéro compte	2 blocs
Montant du dépôt	1 bloc

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 40

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



DES : Data Encryption Standard

- Permutation initiale **PI**



- 16 itérations



$$G_i = D_{i-1}$$

$$D_i = G_{i-1} \oplus f(D_{i-1}, K_i)$$

- Permutation inverse **PI⁻¹**



DES⁻¹ : Il suffit de prendre les clés dans l'autre sens (décalages à droite)

Sélection des clés **K_i** (48 bits)

Clé initiale (56 bits) Permutation **PC1**

$$\Rightarrow (g_0, d_0) \quad (28 \text{ bits} + 28 \text{ bits})$$

Décalages gauches successifs sur g et d, de $k_i \in [1;2]$

$$\Rightarrow (g_i, d_i) \quad (g_{16}, d_{16}) = (g_0, d_0)$$

Permutations avec oubli $\Rightarrow 48$ bits

$$K_i = \text{PC2}(g_i, d_i)$$

Fonction **f**

fonction d'extension **E** : D_{i-1} (32 bits) $\Rightarrow 48$ bits

$$\oplus K_i \text{ (48 bits)} \Rightarrow 8 \text{ blocs de 6 bits}$$

On leur applique les **Sboxes**

(8 boîtes noires : tableaux 4x16 de 4 bits)

Bit 1 et 6 = Numéro de ligne Bit 2 à 5 = Numéro de colonne

On lit 4 bits dans la Sbox \Rightarrow **32 bits résultats**

Cf. Robin ou Beckett ou Schneier

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 41



Génération d'une fonction inversible : Le schéma de Feistel

- Étant donnée une fonction sur n bits, on peut en déduire une fonction inversible sur $2n$ bits

$$\triangleright G_i = D_{i-1}$$

$$\triangleright D_i = G_{i-1} \oplus f(D_{i-1}, K_i)$$

Cette fonction a pour fonction inverse

$$\triangleright D_{i-1} = G_i$$

$$\triangleright G_{i-1} = D_i \oplus f(G_i, K_i)$$

- DES est un schéma de Feistel à 16 étapes
- De nombreux algorithmes de cryptage sont basés sur les schémas de Feistel

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

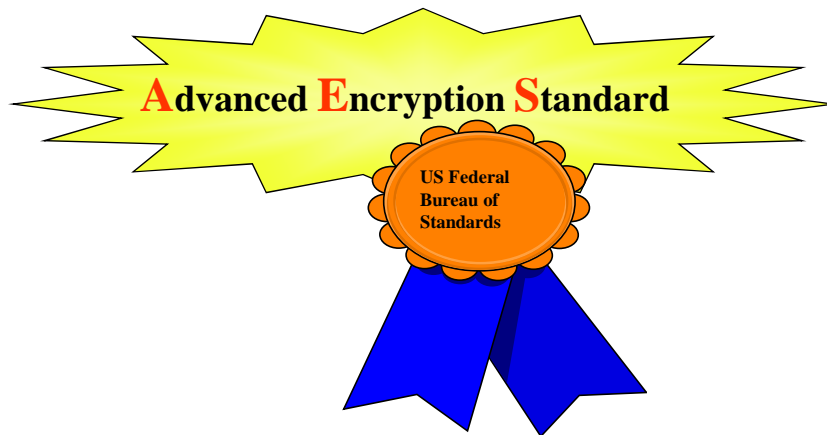
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 42



L'AES

Le nouveau « Standard »



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 43



L'AES

appelé aussi Rijndael

Conçu par Vincent Rijmen et Joan Daemen
Université de Leuven Belgique

Choisi le 2 octobre 2000 par le NIST
(National Institute of Standards and Technology)

- **Plus rapide que le DES**
- **Blocs de 128 bits**
- **Clés de 128, 192 ou 256 bits**
- **Pour le moment aucune faille connue**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 44



L'AES

Principe de base

Le corps de base est un corps fini K à 256 éléments isomorphe à $\{0;1\}[X] / (X^8 + X^4 + X^2 + X + 1)$

Un octet représente un élément de K

- Addition identique à XOR bit à bit
- Multiplication = multiplication de polynômes suivi d'une division euclidienne

Chaque bloc (128 bits = 16 octets) s'écrit comme une matrice (4,4) dont les éléments sont des octets

L'algorithme lui-même

- On additionne une clé secrète au bloc
- On effectue 10 itérations, chacune ayant 4 étapes



L'AES

Une itération = 4 étapes

Un bloc est une matrice (4,4) formée d'éléments de K (octets)

1. Transformation non linéaire S appliquée à chaque octet

2. Décalage des lignes

Permutations circulaires (0,1,2,3) vers la gauche

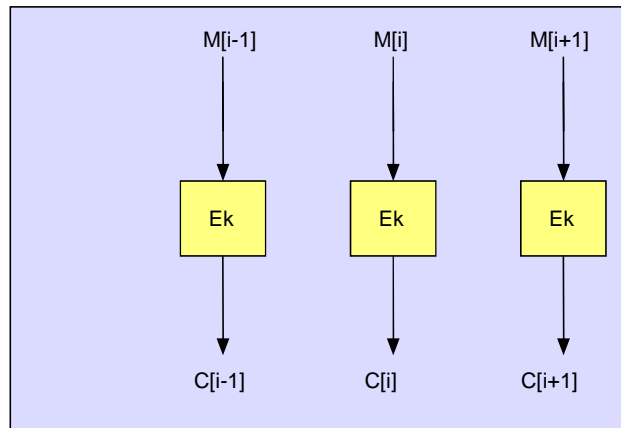
3. Brouillage des colonnes

Multiplication d'une colonne par une matrice (4,4) dont les coefficients sont pris dans {1,2,3}

4. Addition d'une clé de tour (16 octets)

La clé de tour dépend de la clé secrète et est variable d'un tour à l'autre

Mode « standard » EBC



*Risque : l'attaquant peut se constituer un carnet de codage = dictionnaire (Electronic code book)
Possibilité d'attaque par bloc rejoué*

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

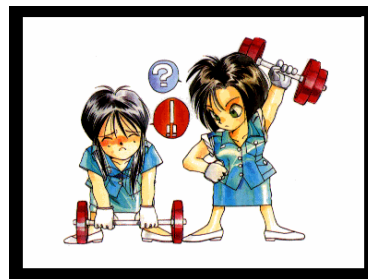
Sécurité des Transactions

30 Avril 2014, page 47

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Amélioration du DES

- *Rendre le chiffrement plus fort*



- Triple DES
- Chaînage des algorithmes par blocs (CBC, CTS, CTR...)

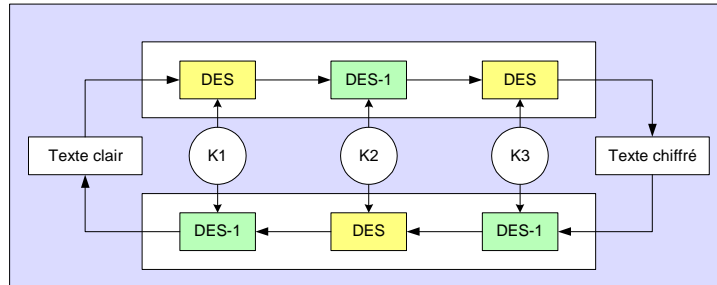
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 48

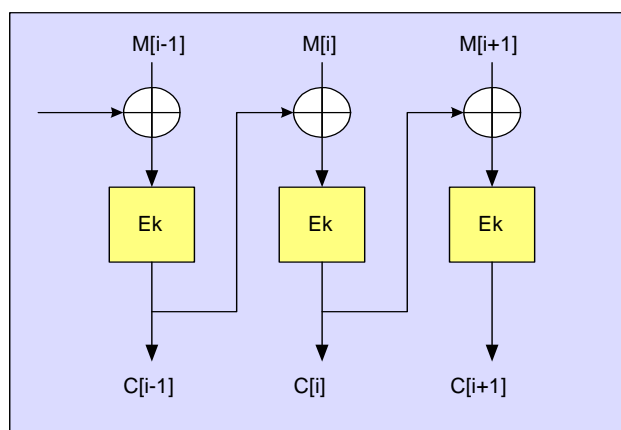
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Triple DES

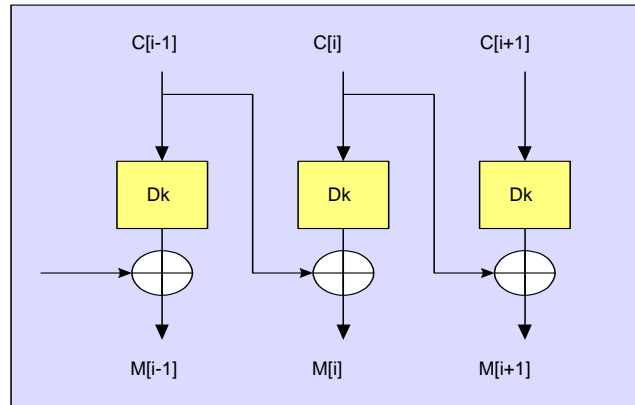


- K1 peut être égal à K3, l'algorithme est alors plus facilement réversible

Mode chaîné CBC



Mode chaîné CBC



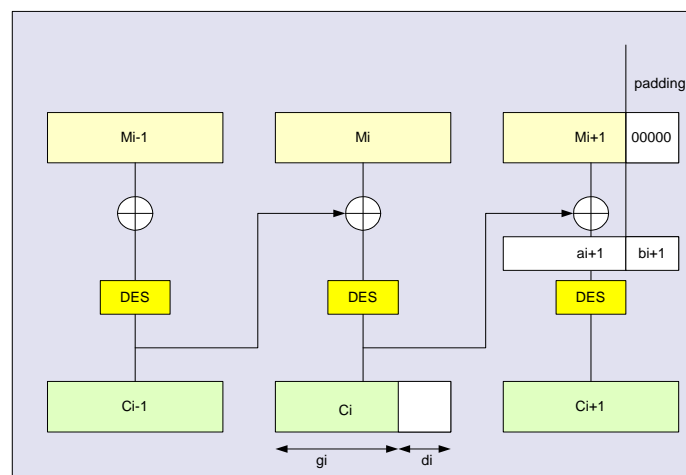
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 51

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Mode chaîné CTS



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 52

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Mode CTR

- On chiffre un compteur, le résultat du chiffrement est XORé avec le texte à chiffrer/déchiffrer

- Chiffrement = déchiffrement
- Pratique pour le chiffrement de supports à accès direct
 - Inutile de tout lire pour déchiffrer un secteur

$$\text{Masque}[n] = \text{AES}_K(f(n))$$

$$\text{CT}[n] = \text{PT}[n] \oplus \text{Masque}[n]$$

Tous ces modes de chaînage sont valables pour tous les algorithmes de chiffrement par blocs

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

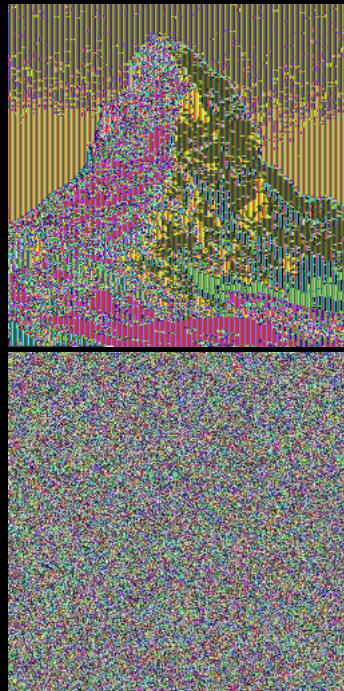
Sécurité des Transactions

30 Avril 2014, page 53

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



**Chiffrement d'une
image en AES
En mode EBC
Avec chaînage**



© Wikipedia

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

30 avril 2014, page 54



Les services d'e-banking

Banque à domicile

- **Problèmes de l'authentification de l'utilisateur**

- ☞ **Comment éviter qu'un pirate se fasse passer pour le client ?**

- ☞ Madame Michu a des compétences limitées en matière de sécurité informatique
 - ☞ Le pirate peut facilement pirater les données d'authentification du client
 - Spyware espionnant les frappes clavier
 - Attaques par phishing

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 55

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les services d'e-banking

Détection du phishing

- **Le phishing**

- ☞ Le pirate simule le faux site bancaires du client
 - ☞ Il reroute le client vers ce site par des mails piégés

- **Comment détecter les phishing ?**

- ☞ **Ne jamais répondre à des demandes envoyées via Internet**

Phishing-Mail vom 4. Juni 2005 /23:17

Von: PostFinance <service@postfinance.ch>

Datum: 4. Juni 2005 23:17:10 GMT+02:00

an: vorname.name@bluewin.ch

Betreff: PostFinance Client - vorname.name@bluewin.ch

Dear PostFinance Customer,

This email was sent by the PostFinance server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your PostFinance online access details. This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it. To verify your e-mail address, click on the link below:

<http://www.postfinance.ch/0QqfV7USKaSZEDQxd3N3c8ZAK9vKdxKRB0BQc7S6mflYqP42wvqLf0gd58s>

Hinter dem Link ist folgendes versteckt:

http://www.google.ca/url?u=http://go.msn.com/HML_6/8.asp?target=http://%09%7165%71cd%69%2E%64%41%72E%75%5d9%52%09%75%5d09

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 56

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les services d'e-banking

Détection du phishing

- **La zone sur laquelle on demande de cliquer est une image**

- ☞ Modification du pointeur de la souris
- ☞ Derrière l'image se cache un site pirate

- **Il y a souvent des textes cachés (blanc sur blanc)**

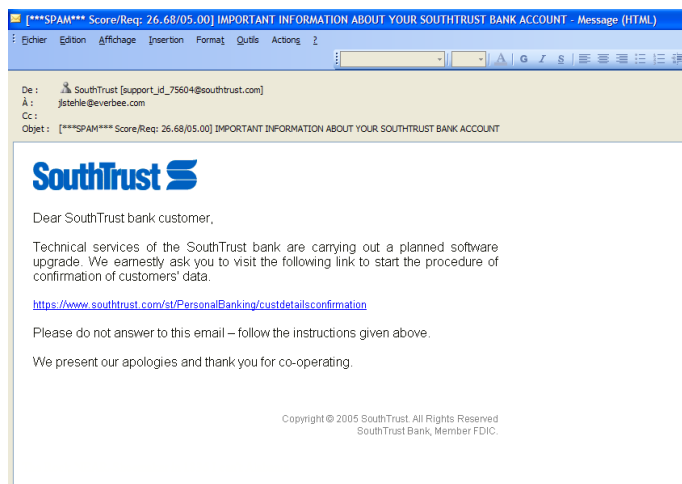
- ☞ Permet de bypasser certains détecteurs de spam
- ☞ Lisible si on les sélectionne à la souris

Quelques exemples



Les services d'e-banking

Détection du phishing





Les services d'e-banking

Banque à domicile Solutions pour authentifier l'utilisateur

- **Login / Password**

- ☞ Très facile à attaquer par spyware

- **Login / Password entré à la souris sur une mire aléatoire**

- ☞ Solution BNP Paribas

- ☞ Attaque possible : le spyware doit récupérer la mire et tous les mouvements de la souris

- **Après Login / Password , utilisation d'un mot de passe à usage unique**

- ☞ Ancienne solution PostFinance Suisse

- ☞ Le client reçoit une petite carte contenant 100 mots de passe, et après l'authentification Login/Password standard, on lui demande un des 100 mots de passe de sa carte

- ☞ Attaque possible : le pirate doit photocopier la carte à l'insu du client

- ☞ **Après Login / Password , Défi/Réponse avec calcul utilisant un pincode.**

SOLUTION ACTUELLEMENT OPTIMALE

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 59

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les services d'e-banking

Banque à domicile Solutions pour authentifier l'utilisateur

Login / Password entré à la souris sur une mire aléatoire

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 60

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les services d'e-banking

Banque à domicile Solutions pour authentifier l'utilisateur

Mot de passe à usage unique

Phase 1 :
Préauthentification

PostFinance - yellownet - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Précédente - - - - - Recherche Favoris

Adresse https://www.yellownet.ch/start_f.html

Deutsch Italiano English PostFinance: Home Contact Aide

PostFinance LA POSTE Une adresse pour votre argent.

yellownet

Login yellownet

Veuillez entrer les éléments de sécurité ci-après:

Numéro yellownet

Mot de passe Suivant

En votre qualité de client possédant une identification d'utilisateur, vous voudrez bien saisir en outre cette dernière.

Identification de l'utilisateur Suivant

Infos sur yellownet

- Info yellownet
- Demo yellownet

Sécurité

- Remarques concernant la sécurité
- La sécurité dans yellownet
- Recommandations de sécurité
- Logiciels de sécurité
- Revoir aux questions (FAQ)

Informations pour la clientèle privée

01.09.2005 > Ouvrez un Compte E-Deposito et recevez CHF 100.-

15.08.2005 > Les bulletins de versement sont menacés d'extinction. Grâce à yellownet, réglez vos factures en trois clics de souris... et participez au concours des dinosaures!

08.08.2005 > Abonnez-vous à la newsletter et gagnez des prix sensationnels!

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 61

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les services d'e-banking

Banque à domicile Solutions pour authentifier l'utilisateur

Mot de passe à usage unique

Phase 2 :
Authentification forte

PostFinance - yellownet - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Précédente - - - - - Recherche Favoris

Adresse https://www.yellownet.ch/start_f.html

Deutsch Italiano English PostFinance: Home Contact Aide

PostFinance LA POSTE Une adresse pour votre argent.

yellownet

Login yellownet

Veuillez indiquer votre numéro de sécurité: access card / liste à biffer no 1, position 18

Numéro de sécurité Transmettre

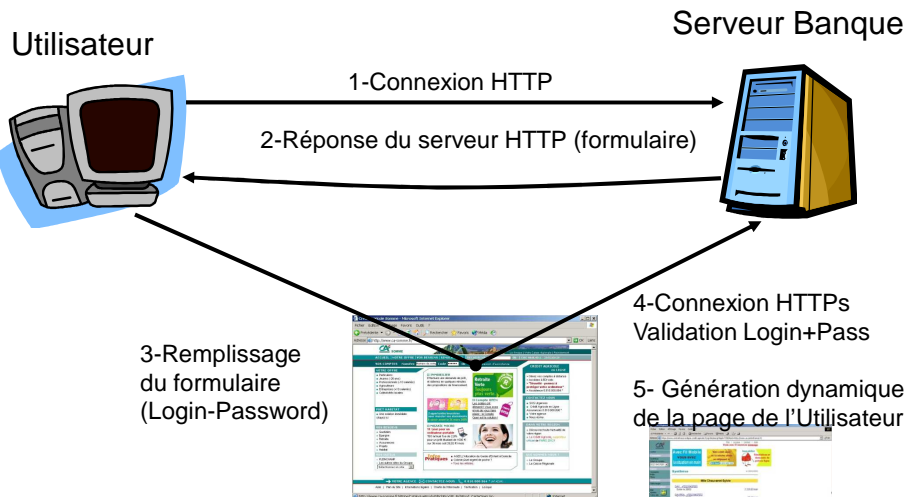
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 62

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Principe général de la connexion Protocole actuel



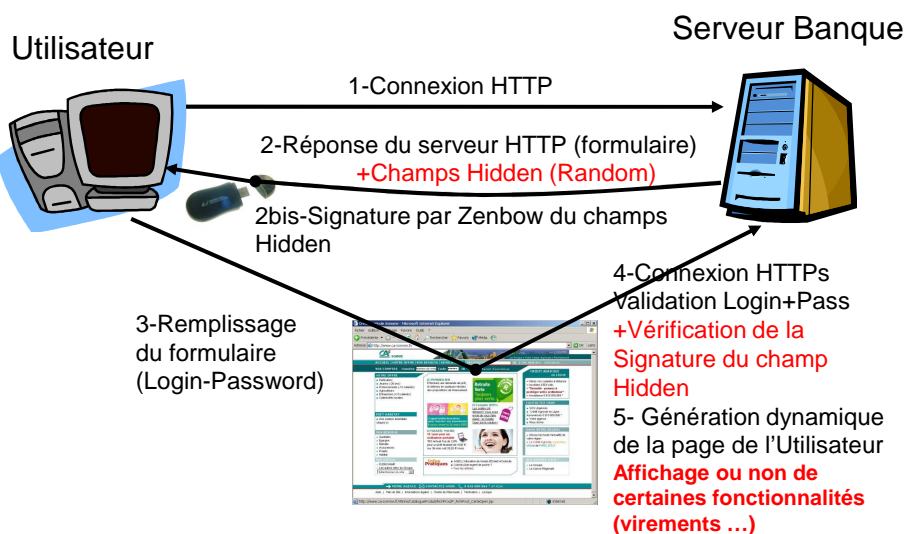
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 63

Principe général de la connexion Technologie Everbee



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

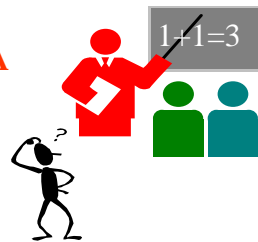
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 64

Et maintenant les détails mathématiques sur

Le logarithme discret
Les nombres premiers
Le théorème d'Euler et RSA

Fonctions à sens unique



Arithmétique modulaire

- **De nombreux systèmes cryptographiques sont basés sur l'arithmétique modulaire**

Logarithme discret

Théorèmes de Fermat et d'Euler

Théorème de Bezout

RSA

- **Propriétés des nombres premiers**
- **Tests de primalité**

- **Développer des algorithmes efficaces en arithmétique modulaire**



Arithmétique modulo N

N est très grand : 1024 bits ($\approx 10^{300}$), 2048, ..., 4096 bits

- **Addition** Facile (Temps en $\log N$)
- **Multiplication** Facile mais plus long ($\log^2 N$)
- **Division** Plus difficile ($\log^3 N$) avec Bezout/Euclide généralisé
- **Réduction modulo N** Il existe des algorithmes de complexité équivalente à celle de la multiplication
- **Puissance a^b** Facile ($\log^3 N$) (écrire b en binaire)



Problème du logarithme Discret

Pas d'algorithme rapide



$$a^x \equiv b [N] ?$$

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Arithmétique Modulaire

30 Avril 2014, page 67

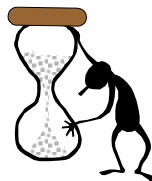
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Problème du logarithme Discret

$$a^x \equiv b [N]$$

- **Pour N grand (10^{300}), le calcul de x connaissant a et b nécessite un temps supérieur à l'âge de l'univers**



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

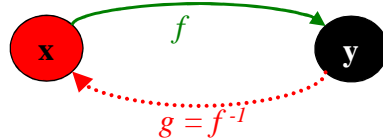
Sécurité des Transactions

30 Avril 2014, page 68

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



L'exponentiation modulaire est une fonction à sens unique



a et N sont connus et publics

– $y = f(x) = a^x \pmod{N}$

– $x = g(y)$ est la solution, en arithmétique modulo N de l'équation $a^x = y$ (Logarithme discret en base a)

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Arithmétique Modulaire

30 Avril 2014, page 69

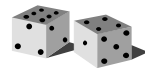
Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Diffie Hellman : Échange de clé sur un réseau public



- N et $g \in (\mathbb{Z}/N\mathbb{Z})^*$ (Problème du choix de g)
- Alice calcule a aléatoire, envoie $g^a[N]$
- Bob calcule b aléatoire, envoie $g^b[N]$
- Les deux peuvent calculer $g^{ab}[N]$
- Le pirate connaît g $g^a[N]$ $g^b[N]$



mais ne peut pas calculer $g^{ab}[N]$

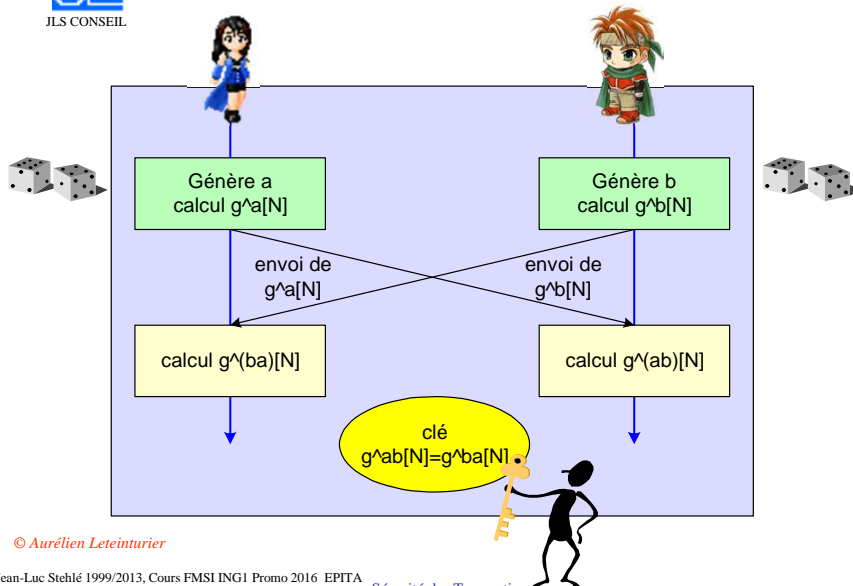
© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 70

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Protocole de Diffie-Hellman



Faibles / Backdoors dans le problème du logarithme discret

- **Groupes faibles**
- **Groupes choisis intentionnellement pour créer un backdoor**
 - **Utiliser des groupes « aléatoires »**
 - **Les groupes d'Oakley**
Basés sur les décimales de π



Les groupes d'Oakley

• Groupe 1 : 768 bits

$2^{768} - 2^{704} - 1 + 2^{64} \times [149686 + 2^{638}\pi] =$
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A63A3620 FFFFFFFF FFFFFFFF



Les groupes d'Oakley

• Groupe 2 : 1024 bits

$2^{1024} - 2^{960} - 1 + 2^{64} \times [129093 + 2^{894}\pi] =$
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE65381
FFFFFFFF FFFFFFFF



Les groupes d'Oakley

• Groupe 5 : 1536 bits

$2^{1536} - 2^{1472} - 1 + 2^{64} \times [741804 + 2^{1406}\pi] =$

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D
670C354E 4ABC9804 F1746C08 CA237327 FFFFFFFF FFFFFFFF

© Jean-Luc Stehlé 1999/2013, Cours FMSI INGI Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 75

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Les groupes d'Oakley

• Principe de construction (exemple 768 bits)

➤ $(2^{64}-1) \times (2^{704}+1) = 2^{768} - 2^{704} + 2^{64} - 1 =$

FFFFFFFF FFFFFFFF 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 FFFFFFFF FFFFFFFF

➤ On complète par le développement binaire de π entre les bits 704 = 768-64 et 64



C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA237327 FFFFFFFF FFFFFFFF
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED DE2BCBFE 95581718 3955497C 8A956A85 15D22618 98FA0510
15728E5A 8AAAC2DD AD33170D 04507A33 AB5521AB DFCBA644 ECFB8504 5BDB8F0A 8A8A7157 D0460C7D B3970985 A6E1E4C7
A8F5A8EC D80933D7 18C9C480 4A25619D CE83D226 1AD28E6B F12FFA06 D98A0864 D8760273 38C8A6A4 52192818 177B200C
BBE11757 7A615D6C 770989C0 BAD946E2 08E24FA0 7485AB31 43DB5BFC B0FD108E 4B82D120 A9210801 1A723C12 A787E6D7
8B719A10 B0BA5B26 99C32718 6A44823C 1A946834 861508DA 25B385CA 2AD44CEB 08B8C2D8 0418B8F9 2B8BF1C4 1F8E2AA6
287C5947 486C0C5D 99B2964F A090C3A2 2338A186 6158B7ED 1F612970 CE82D7AF B81BD076 2170481C D0069127 D5B05AA9
93B48A98 8D8FDDC1 86FFB7DC 90A6C08F 4DFA35C9 34028492 36C3FAB4 D27C7026 C1D4DCB2 602646DE C9751E76 3DBA37BD
F8FF9406 AD9E530E 85DB382F 413001AE B06A53BD 9027D831 17972780 865A8918 DA3EDBEB CF9B14ED 44C8E6CA CED48B1B
DB7E1447 86CC254B 33205151 28078A42 69B8F4C1 378C2D8F 59B3CA01 C648B2BC F032AA15 D1721D03 F482D7C8 6874F8F6
D55E702F 46980C82 85A84031 900B1C9E 59E7C97F B8C788F3 23A97A7E 36CC88BE 0F1D45B7 FF585AC5 4BD407B2 2B4154AA
CC896D7E B748E1D8 14CC58D2 0F80378D A797158E F298E328 06A1D58B B7C5DA76 F550AA3D 8A1F8F90 B819CCB1 A313D55C
DA56C98C 2BF29632 3B7FE8D7 6E3C9468 043E8F66 F4F460EE 12B82D5B 0B7474D6 8694F91E 4DBE1159 74A3926F 12FE58A
38777CB6 A932D9FC DB8EC4D0 73B931BA 38C832B6 ED9D0300 741FA7BF 8AFC47ED 2576F693 68A42466 3AAB39C 5A84F568
3423B474 2BFC1C978 238F16CB E39D652D E3FDB8BE FC848AD9 22222B04 A4037C07 13B857A8 1A23F0C7 3473FC64 6CEA306B
4BC8C866 2F8385DD FAD04B7F A2C087B8 79683303 BDB8DD3A 062B3CF5 B3A27BA6 62A13F8 3F44F92D DF310E8D 7A8BA3A6
45978B99 A02550C1 64F31C5C 0846851D F0A84819 5DB78A1 B1D510B0 78E74D73 FAF36BC3 18C7A268 359464F4 B8B79F92
400943BB 481CCD7 889A002E D5E8382B C9190DA6 FC026E47 9558E447 5677E9AA 9E3050E2 765694D0 C81F56E8 80B96E71

➤ On recherche le premier nombre p supérieur à cela, premier tel que (p-1)/2 soit lui-même premier (nombre de Sophie Germain) et dont les 64 bits de poids faible soient à 1

➤ D'où le résultat $2^{768} - 2^{704} - 1 + 2^{64} \times [149686 + 2^{638}\pi]$

© Jean-Luc Stehlé 1999/2013, Cours FMSI INGI Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 76

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



La génération des nombres aléatoires

- Indispensables pour les schémas de Diffie-Hellman
 - Utilisés dans les protocoles IPSec
 - **Peuvent être utilisés pour créer des masques XOR**
 - Utilisés pour les générations automatiques de clés
 - L'exemple de PGP
- La génération de nombres aléatoires introduit une faille dans la méthode*

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 77

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



La génération des nombres aléatoires

- La suite des aléas générés doit ressembler à une suite « au hasard »
 - Équiprobabilité de tous les motifs possibles*
 - Tests statistiques*
- La suite des aléas générés doit être parfaitement imprévisible pour le pirate
- **Notion d'entropie des nombres aléatoires**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 78

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



La génération des nombres aléatoires

- **Générateurs aléatoires purs :**
basés sur un phénomène aléatoire
 - *Bruits de fond d'un circuit électronique*
 - *Diode Zener au point d'instabilité*
 - *Trafic sur un réseau informatique*
 - *Checksum de la mémoire vive*
- **Générateurs pseudo-aléatoires :**
basés sur un algorithme mathématique
parfaitement déterministes



Les générateurs pseudo-aléatoires

- **Notion d'automate fini**
 - **État de l'automate**
 - **Algorithme fournissant**
 - *Résultat pour calculer le prochain nombre aléatoire*
 - *Nouvel état*
 - **Périodique**
- **Exemple : « The bad and dirty generator »**
$$x \leftarrow x \times 7^5 \text{ [Mod } M_{31}]$$
$$M_{31} = 2^{31} - 1 : \text{Nombre premier de Mersenne}$$
- *La connaissance d'un résultat permet de calculer intégralement tout le passé et tout le futur*



Les générateurs pseudo-aléatoires

- « Camoufler » l'état du générateur
 - Appliquer un DES_k au résultat du générateur
 - Utiliser un shuffle
- Mettre en parallèle plusieurs générateurs désynchronisés pour augmenter la périodicité
 - Générateur de période très grande ($>$ âge de l'univers)
 - Perturbation par des aléas vrais
- Brevets Everbee sur les générateurs aléatoires

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

30 Avril 2014, page 81



Diffie Hellman : Échange de clé sur un réseau public



Peut être attaqué par le « man in the middle »



© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

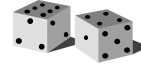
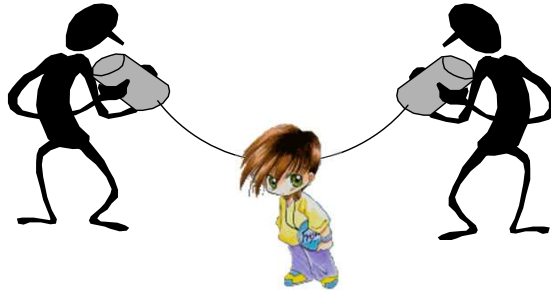
30 Avril 2014, page 82



Diffie Hellman : Échange de clé sur un réseau public



Peut être attaqué par le « man in the middle »



**Parade : Sécuriser l'échange D-H
par un chiffrement asymétrique**

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 83

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Complexité algorithmique

**Temps de calcul en fonction du nombre n de bits
des données**

Algorithmes polynomiaux

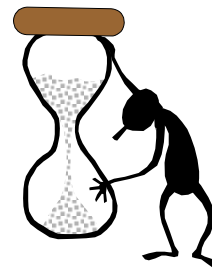
- Linéaires (addition)
- Quadratiques (multiplication)
- Cubiques (exponentiation)

Algorithmes exponentiels

- Casser le Log discret par attaque brutale
(essayer successivement tous les exposants)

Algorithmes subexponentiels

- $L_n(\gamma, c) = O(\exp(c \cdot n^\gamma \ln(n)^{1-\gamma}))$
- $\gamma=1$: exponentiels $\gamma=0$: polynomiaux



Log discret : $\gamma=1/2$ et depuis les théories du crible numérique de Lenstra (1993) $\gamma=1/3$

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 84

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



A propos des ordres de grandeur

Hypothèse : processeur à 1 GHz

- 1 seconde = 10^9 nanosecondes $\approx 2^{30}$ nanosecondes
- 1 jour = 86400 secondes $\approx 2^{16}$ secondes.
- 1 an = 365.25 jours = 31 557 600 secondes
 $\approx 2^{25}$ secondes $\approx 2^{55}$ nanosecondes
- Âge de l'univers ≈ 20 milliards d'années
 $\approx 6.10^{17} \approx 2^{59}$ secondes $\approx 2^{89}$ nanosecondes

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 85

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



A propos des ordres de grandeur

Application cryptographiques (processeur à 1GHz)

	Nombre de tops d'horloge	Log base 10	Log base 2
1 seconde	1.000E+09	9.000	29.897
1 jour	8.640E+13	13.937	46.296
1 an	3.154E+16	16.499	54.808
Grid pendant 1 jour (un milliard de CPU à 1GHz)	8.640E+22	22.937	76.193
Grid pendant 1 an (un milliard de CPU à 1GHz)	3.154E+25	25.499	84.705
Grid pendant 20 milliards d'années (un milliard de CPU à 1GHz)	6.307E+35	35.800	118.924
Grid pendant 20 milliards d'années (un milliard de CPU à 10TFlops)	6.307E+39	38.800	128.890

Rappel :

- DES = 56 bits
- Triple DES = 112 bits
- Algo actuels = 128 bits

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 86

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Accélérateurs d'attaques

On se propose de casser le Log discret

- Déterminer a connaissant g^a [modulo N]

- Si on a le temps

- Essayer tous les a possibles
- En moyenne il faudra $N/2$ essais

- Si on a la mémoire

- Calculer une fois pour toutes tous les g^a [modulo N]
- Les stocker en mémoire (fichiers indexés...)
- Pour chaque nouveau g^a consultation de table

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 87

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Accélérateurs d'attaques

On se propose de casser le Log discret

- Déterminer a connaissant g^a [modulo N]

- Attaque mixte

- Précalculer et stocker g^a [modulo N]
pour T valeurs de a équiréparties (*distantes de S avec $S.T=N$*)
- Etant donné un g^a avec a inconnu,
s'il n'est pas dans la table, multiplier par g et réitérer
jusqu'à trouver un élément présent dans la table
En moyenne $S/2$ calculs
- *Exercice : Quel est le γ ?*

- Exemple numérique : $N \approx 10^{18} \approx 2^{60}$

- Précalculer et stocker 10^9 valeurs : Quelques gigas de mémoire
- En moyenne un demi milliard de calculs suffisent...

- Les ressources nécessaires au pirate croissent comme la racine carrée de N

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 88

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Applications du Logarithme Discret

- Il est impossible d'inverser en un temps raisonnable l'exponentiation modulaire

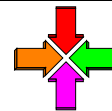
Protocoles d'échanges de clés (Diffie Hellman)

Chiffrement asymétrique (El Gamal)

Protocoles d'authentification



Système de El Gamal



- Système de chiffrement asymétrique

Tout le monde peut envoyer un message secret à A

N et g sont publics (*N premier, g générateur de $\mathbb{Z}/N\mathbb{Z}$*)

A choisit a aléatoire secret et publie $g^a \text{ [Mod N]}$

– $g^a \text{ [Mod N]}$ est la clé publique de A

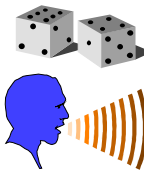
Pour envoyer un message M à A,

B génère un k aléatoire secret, et envoie

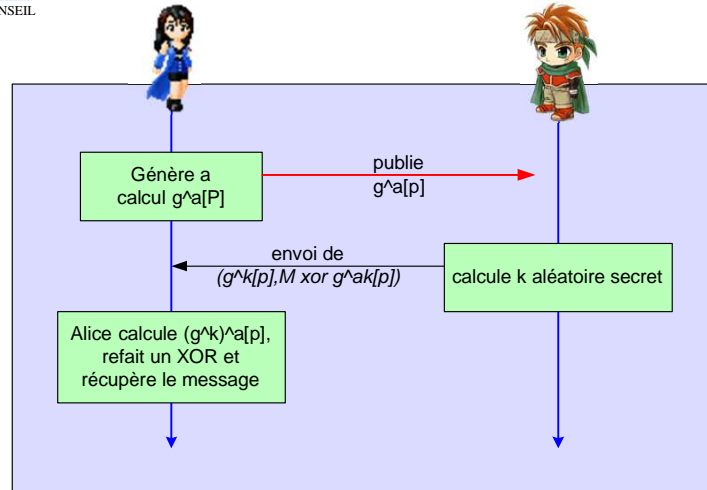
$(g^k \text{ [Mod N]}, M \oplus g^{ak} \text{ [Mod N]})$

A calcule $(g^k)^a \text{ [Mod N]}$ et refait un \oplus pour retrouver M

- Le pirate connaît g [Mod N], $g^k \text{ [Mod N]}$ et $g^a \text{ [Mod N]}$ mais il n'a aucun moyen de retrouver $g^{ak} \text{ [Mod N]}$



Système de El Gamal



© Aurélien Leteinturier

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 91

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document

Un protocole d'authentification

• Protocole de défi/réponse (Similaire à El Gamal)

N et g sont publics (N premier, g générateur de $\mathbb{Z}/N\mathbb{Z}$)

A choisit a aléatoire secret et publie $g^a \pmod{N}$

- a est la clé secrète de A
- $g^a \pmod{N}$ est la clé publique de A

Pour authentifier A,

- B génère un k aléatoire secret,
- calcule g^k
- envoie g^k à A (c'est le *défi*)

A calcule $(g^k)^a$ et le renvoie à B (c'est la *réponse* au défi)

**• Le pirate connaît g , $g^k \pmod{N}$ et $g^a \pmod{N}$
mais il n'a aucun moyen de retrouver $g^{ak} \pmod{N}$**

• Seul quelqu'un connaissant a pouvait répondre correctement au défi

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 92

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Protocole de Défi / Réponse

- **Pour authentifier A, on lui envoie un défi**
- **Seul quelqu'un connaissant la clé secrète de A peut calculer rapidement la réponse**
 - Le calcul de la réponse nécessite une exponentiation modulaire
- **Un pirate ne connaissant pas la clé secrète doit faire un calcul très long**
 - Il faut résoudre le logarithme discret
- **A dispose d'une puissance de calcul limitée**
 - carte à puce, carte SIM de téléphone mobile
- **Le pirate dispose de moyens très importants**
 - organisation criminelle puissante

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 93

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document



Bonnes fonctions à sens unique ?

- **C'est un des enjeux des recherches actuelles**
 - Fonction directe rapide à calculer sur des processeurs à très faible puissance**
 - Fonction inverse impossible à calculer même avec des ressources puissantes**
- **En tenant compte des possibles évolutions de la technologie et des puissances de calcul**
- *Utilisation de courbes elliptiques sur un corps fini*
- *Groupes de Jacobi des courbes hyperelliptiques*

© Jean-Luc Stehlé 1999/2013, Cours FMSI ING1 Promo 2016 EPITA

Sécurité des Transactions

30 Avril 2014, page 94

Document destiné uniquement aux élèves et aux enseignants de l'EPITA. L'auteur vous remercie d'avance de ne pas diffuser ce document