

Cryptologie & Sécurité

Master 1 informatique

Université Claude Bernard Lyon 1

Fabien LAGUILLAUMIE

fabien.laguillaumie@ens-lyon.fr

<http://perso.ens-lyon.fr/fabien.laguillaumie>





Introduction

Recommandations sur la taille des clés

Histoire

L'âge artisanal

L'âge technique

L'âge paradoxal

Les objectifs de la cryptographie

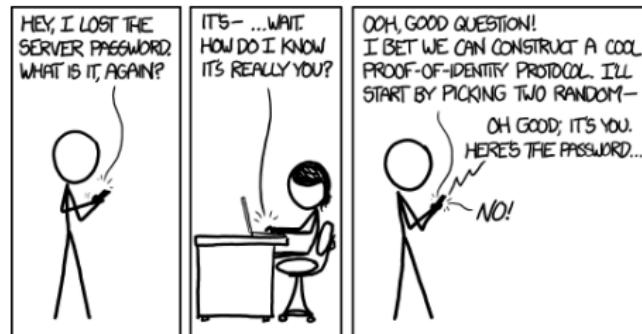
Confidentialité

Chiffrements historiques

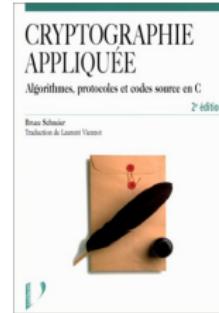
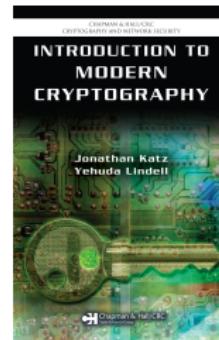
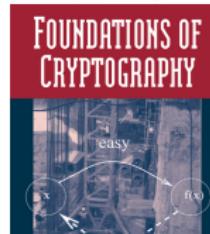
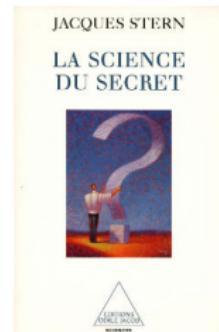
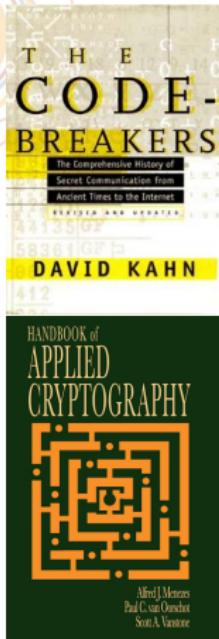
Introduction



LA CRYPTOGRAPHIE



Bibliographie



Introduction

Cryptologie = science du secret et de la confiance

► Oded Goldreich (Weizmann Institute of Science) :

« Cryptography is concerned with the construction of schemes that withstand any abuse : Such schemes are constructed so to maintain a desired functionality, even under malicious attempts aimed at making them deviate from their prescribed functionality. »



Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

▶ Internet :

- ▶ sites bancaires
- ▶ sites de vente en ligne
- ▶ site d'enchères
- ▶ ...



Introduction

Dans la vraie vie :

- ▶ Carte à puce
- ▶ cartes de paiements
- ▶ carte vitale



Introduction

Dans la vraie vie :



- ▶ Signature électronique (<http://www.ssi.gouv.fr>)

La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire.

L'**écrit électronique signé électroniquement peut être reconnu comme preuve en justice**. L'ANSSI a publié un mémento visant à dresser le cadre juridique autour de la signature électronique. Partant d'un rappel sur le contexte législatif, il expose, au jour d'aujourd'hui, le cadre technique défini pour la mise en œuvre d'une signature électronique présumée fiable au sens du décret 2001-272 sur la signature électronique.

Pour l'ensemble du vocabulaire utilisé dans ce document il est conseillé de se référer à la FAQ « Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ».

Le procédé de signature électronique est présumé fiable, au sens du décret 2001-272 sur la signature électronique, si :

- ▶ la signature électronique est sécurisée ;
- ▶ elle est créée par un dispositif sécurisé de création de signature, c'est à dire par un dispositif certifié conforme aux exigences de l'article 3. I du décret conformément à la procédure de "Certification de conformité des dispositifs de création de signature électronique" ;
- ▶ et la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié. Les certificats délivrés par des "prestataires de services de certification électronique qualifiés" sont présumés qualifiés.

Introduction

Dans la vraie vie :



PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Signature électronique Point de situation

MEMENTO

Version 0.94
25.08.04

Introduction

Dans la vraie vie :

- ▶ Vote électronique
- ▶ machines à voter
- ▶ vote en ligne

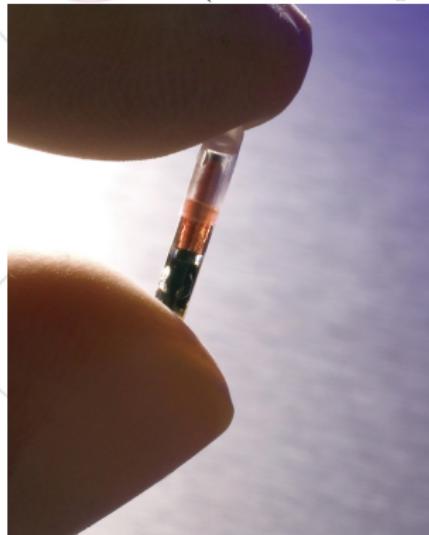


Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

- ▶ RFID (Radio-Frequency IDentification)



Source : www.avoine.net/gratis

- ▶ RFID Security & Privacy Lounge
<http://www.avoine.net/rfid/>

Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :



Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :

- ▶ identification animale
- ▶ identification VIP



Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :



Introduction

Cryptologie = science du secret et de la confiance

Dans la vraie vie :



Relay Attacks on Passive Keyless Entry and
Start Systems in Modern Cars

Aurélien Francillon, Boris Danev, Srdjan Čapkun

Department of Computer Science

ETH Zurich

8092 Zurich, Switzerland

{aurelien.francillon, boris.danev, srdjan.capkun}@inf.ethz.ch

Introduction

Dans la vraie vie :

- ▶ Télé payante
- ▶ décodeur
- ▶ pay-tv



Introduction

Dans la vraie vie :

- ▶ Télécommunications
- ▶ GSM
- ▶ Wifi



- ▶ Hybrid fixed/mobile phone enabling communications both over fixed (PSTN, ISDN, VoIP) and mobile (Quadri-Band GSM, GPRS Class 10, EDGE, UMTS) telecom networks
- ▶ Vocoders ensuring secure and high-quality speech : STANAG 4591 (2.4 kbps) and G.728 (16 kbps)
- ▶ Security level : High Grade (up to French « SECRET DÉFENSE »)

Introduction

► Mail à la liste Crypto de l'ÉNS (16 août 2010) : Vodafone Mobile Algorithms

New Mobile Phone Security Algorithms - Public Evaluation Invited

A new set of cryptographic algorithms is being proposed for inclusion in the "4G" mobile standard called LTE (Long Term Evolution).

The algorithms are :

- * a stream cipher called ZUC, which is the core of both new LTE algorithms ;
- * the LTE encryption algorithm called 128-EEA3, defined straightforwardly using ZUC ;
- * the LTE integrity algorithm called 128-EIA3, designed as a Universal Hash Function using ZUC as its core.

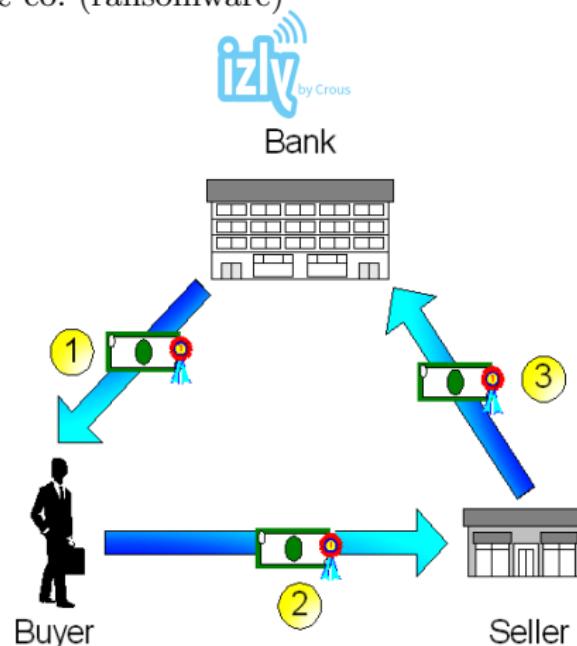
The algorithms are here : http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm. All of the algorithms were designed by DACAS, the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences. They have been evaluated by the algorithm standardisation group ETSI SAGE, and also by two other teams of well known cryptologists, and are believed to be strong and suitable for LTE.

Now the algorithms are open for public evaluation. Comments and analysis are invited, before a final decision is taken in (probably) January 2011 as to whether to include the new algorithms in the LTE standard. A discussion forum <http://zucalg.forumotion.net/> has been created for this - please post any evaluation results there.

Introduction

Dans la vraie vie :

- ▶ Paiement
- ▶ Porte-monnaie électronique
- ▶ e-cash
- ▶ Bitcoin & co. (ransomware)



Introduction

The New York Times

SEARCH

EDITORIAL
Leaving the E.U. Would Hurt Britain's Economy

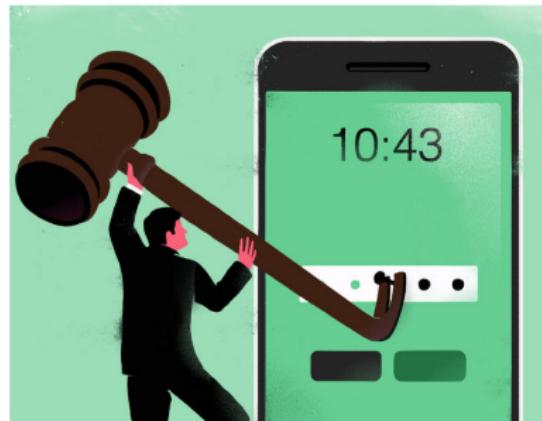
CHARLES M. BLOW
The End of American Idealism

PAUL KRUGMAN
When Fallacies Coll

The Opinion Pages OP-ED CONTRIBUTORS

When Phone Encryption Blocks Justice

By CYRUS R. VANCE Jr., FRANÇOIS MOLINS, ADRIAN LEPPARD and JAVIER ZARAGOZA AUG. 11, 2015



François Molins: "Les nouveaux téléphones rendent la justice aveugle"

Actualité | Société | Propos réactualisés par Emmanuel Paquette et Eric Peltier; publiés le 02/09/2015 à 08:57

521



TRIBUNE

Sécurité informatique : tous connectés, tous responsables

Par Guillaume Pospard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) — 21 janvier 2016 à 08:39 (mis à jour le 22 janvier 2016 à 12:31)



Partager

Tweeter

Introduction

Google News : cryptograph(y/ie)



USB-C upgrade allows cryptography to authenticate connected devices

Ben Lovejoy - Jan 2nd 2019 7:45 am PT [@benlovejoy](#)



Protection des données : débattre pour résoudre la «crise de confiance»

Par Amélie Dubois -- 30 Janvier 2018 à 11:40

SHARES PARTAGER TWITTER

Forbes BILLIONAIRES Innovation Leadership Money Consumer Industry

3,949 views | Jan 12, 2019, 04:34pm

IBM Lattice Cryptography Is Needed Now To Defend Against Quantum Computing Future

Kevin Krewell Contributor
Tirias Research Contributor Group
Enterprise & Cloud

When it comes to securing data, it is not too early to start anticipating the future threat of quantum computing. Today's cryptographic

DARKReading | Join us live at Interop

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

ANALYTICS ATTACKS/BREACHES APP SEC CAREERS & PEOPLE CLOUD ENDPOINT IoT MOBILE OPERATIONS

ATTACKS/BREACHES

12/22/2019
6:26 PM

The Fact and Fiction of Homomorphic Encryption



The approach's promise continues to entice cryptographers and academics. But don't expect it to help in the real world anytime soon.

The history of homomorphic encryption stretches back to the late 1970s. Just

Introduction

Le cœur de la crypto :

- ▶ échange de clés
- ▶ sécurité des communications (confidentialité, intégrité)



Introduction

Le cœur de la crypto :

- ▶ échange de clés
- ▶ sécurité des communications (confidentialité, intégrité)

mais encore

- ▶ signatures numériques
- ▶ communications anonymes
- ▶ protocoles : vote, e-cash, enchères, interrogation anonyme de BD
- ▶ **multi-party computation** (thm : c'est possible !)



Introduction

Le cœur de la crypto :

- ▶ échange de clés
- ▶ sécurité des communications (confidentialité, intégrité)

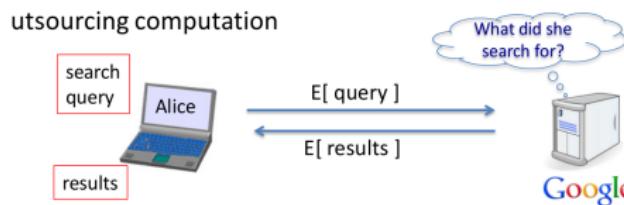


mais encore

- ▶ signatures numériques
- ▶ communications anonymes
- ▶ protocoles : vote, e-cash, enchères, interrogation anonyme de BD
- ▶ **multi-party computation** (thm : c'est possible !)

et la magie :

- ▶ preuves à divulgation nulle de connaissance
- ▶ calculs secrets délégués



Multiparty computation



- ▶ Alice et Bob ont eu un premier rendez-vous
- ▶ Ils veulent savoir s'il y en aura un second
mais...

ils ne veulent pas se prendre une veste en direct !

- ▶ Ils vont jouer à un jeu à l'issue duquel, la seule information connue sera la possibilité d'un second rendez-vous ou pas.

Multiparty computation



- ▶ Alice et Bob ont eu un premier rendez-vous
- ▶ Ils veulent savoir s'il y en aura un second
mais...

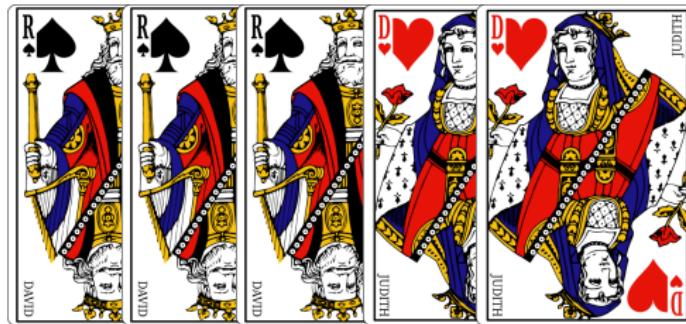
ils ne veulent pas se prendre une veste en direct !

- ▶ Ils vont jouer à un jeu à l'issue duquel, la seule information connue sera la possibilité d'un second rendez-vous ou pas.

Après le premier rendez-vous :

- ▶ Alice sait si elle veut un second rendez-vous
- ▶ Bob sait si il veut un second rendez-vous
- ▶ et c'est tout !

Multiparty computation



Multiparty computation

Dans ce jeu :

- ▶ Un **roi** de ♠ est face cachée sur la table
- ▶ Alice et Bob reçoivent un **roi** et une **reine**
- ▶ Bob pose ses cartes face cachée par dessus le **roi** de ♠
 - ▶ si il veut un second rendez-vous : **reine** au dessus
- ▶ Alice pose ses cartes face cachée sur le dessus du paquet
 - ▶ si elle veut un second rendez-vous : **roi** sur le dessus



Multiparty computation

Dans ce jeu :

- ▶ Un **roi** de ♠ est face cachée sur la table
- ▶ Alice et Bob reçoivent un **roi** et une **reine**
- ▶ Bob pose ses cartes face cachée par dessus le **roi** de ♠
 - ▶ si il veut un second rendez-vous : **reine** au dessus
- ▶ Alice pose ses cartes face cachée sur le dessus du paquet
 - ▶ si elle veut un second rendez-vous : **roi** sur le dessus



Multiparty computation

Dans ce jeu :

- ▶ Un **roi** de ♠ est face cachée sur la table
- ▶ Alice et Bob reçoivent un **roi** et une **reine**
- ▶ Bob pose ses cartes face cachée par dessus le **roi** de ♠
 - ▶ si il veut un second rendez-vous : **reine** au dessus
- ▶ Alice pose ses cartes face cachée sur le dessus du paquet
 - ▶ si elle veut un second rendez-vous : **roi** sur le dessus



Multiparty computation

Dans ce jeu :

- ▶ Un **roi** de ♠ est face cachée sur la table
- ▶ Alice et Bob reçoivent un **roi** et une **reine**
- ▶ Bob pose ses cartes face cachée par dessus le **roi** de ♠
 - ▶ si il veut un second rendez-vous : **reine** au dessus
- ▶ Alice pose ses cartes face cachée sur le dessus du paquet
 - ▶ si elle veut un second rendez-vous : **roi** sur le dessus



- ▶ Alice et Bob coupent

Multiparty computation

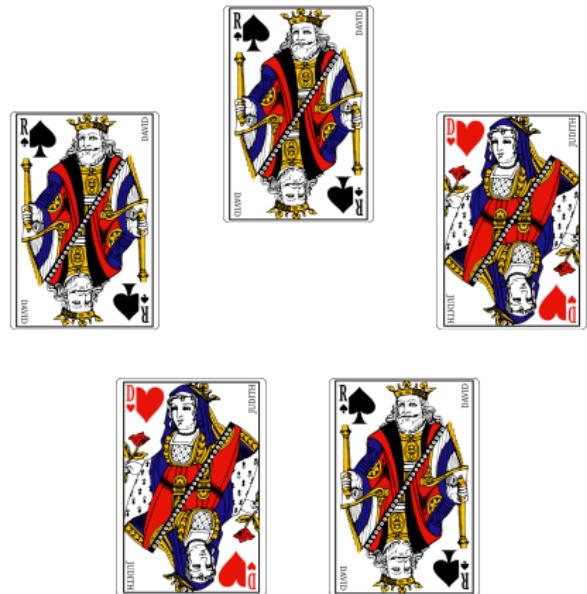
- ▶ Si les reines sont côté à côté :
Alice et Bob sont amoureux !



Multiparty computation

- ▶ Si les reines sont côté à côté :
Alice et Bob sont amoureux !

- ▶ Sinon :
Rien n'est révélé si les reines ne sont pas côté à côté

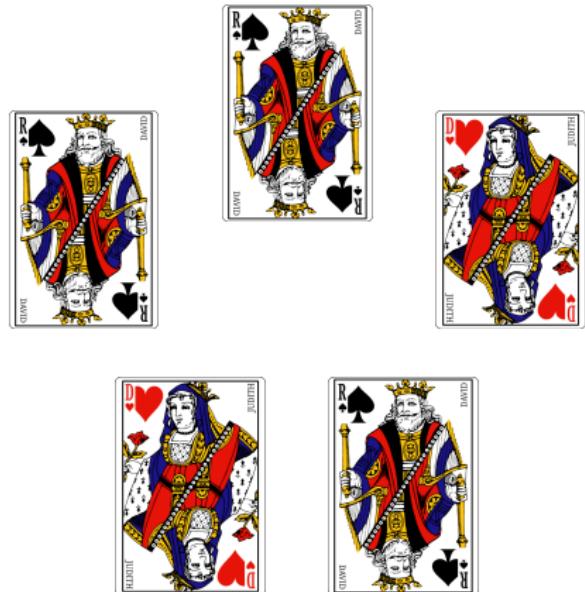


Multiparty computation

- ▶ Si les reines sont côté à côté : Alice et Bob sont amoureux !

- ▶ Sinon :
Rien n'est révélé si les reines ne sont pas côté à côté

i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment



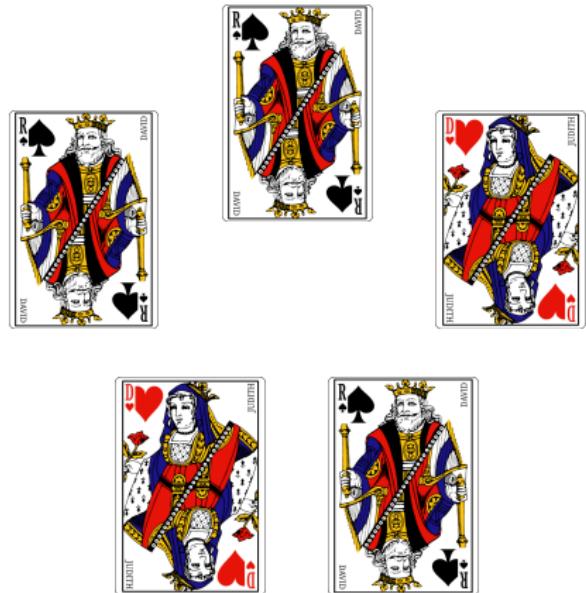
Multiparty computation

- ▶ Si les reines sont côté à côté : Alice et Bob sont amoureux !

- ▶ Sinon :
Rien n'est révélé si les reines ne sont pas côté à côté

i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment

- ▶ fonction “et”



Multiparty computation

- ▶ Si les reines sont côté à côté :
Alice et Bob sont amoureux !

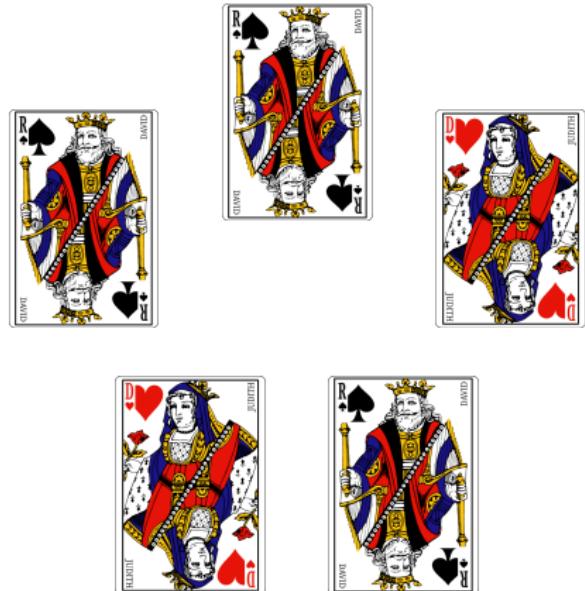
- ▶ Sinon :
Rien n'est révélé si les reines ne sont pas côté à côté

i.e., on ne sait pas si seul l'un des deux n'aime pas l'autre, ou aucun ne s'aiment

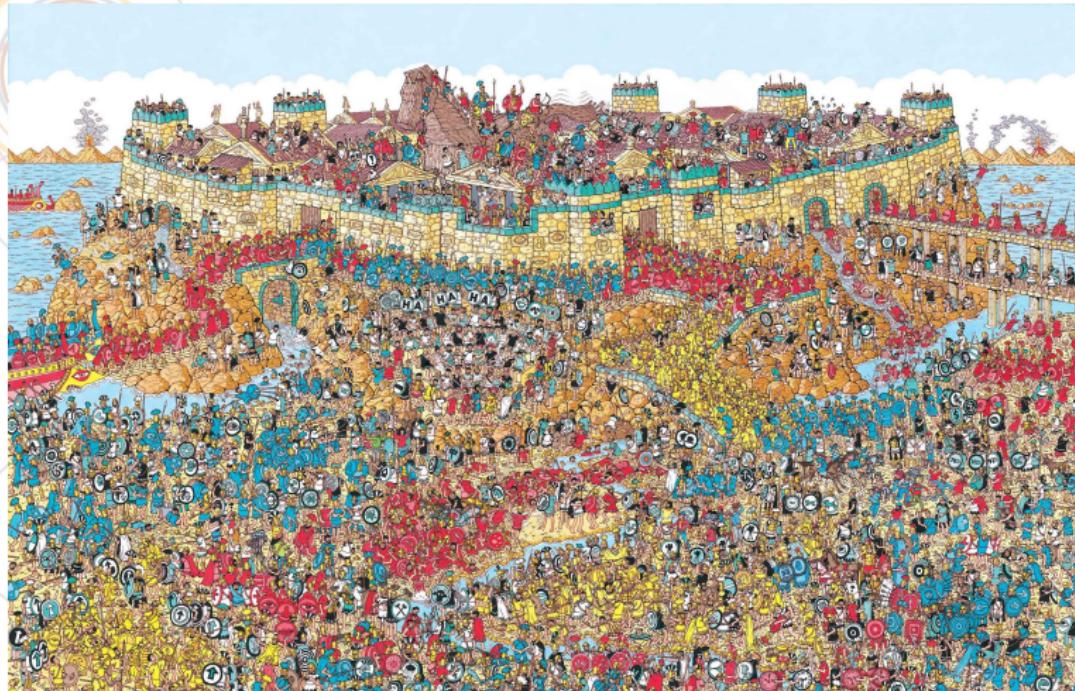
- ▶ fonction “et”

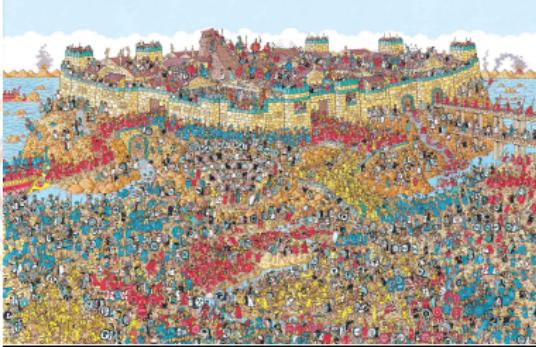
Multiparty computation : calcule une fonction de sorte à ce qu'une entrée secrète ne soit pas révélée aux autres parties

(attention : de l'information peut se déduire du résultat de la fonction)

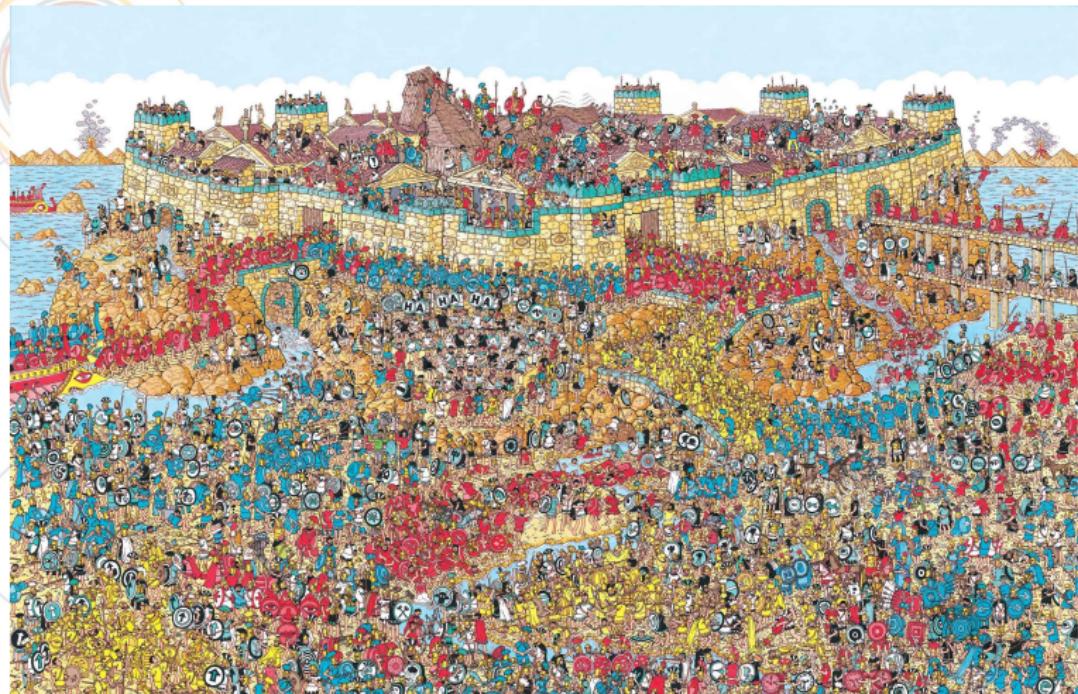


Introduction : zero-knowledge

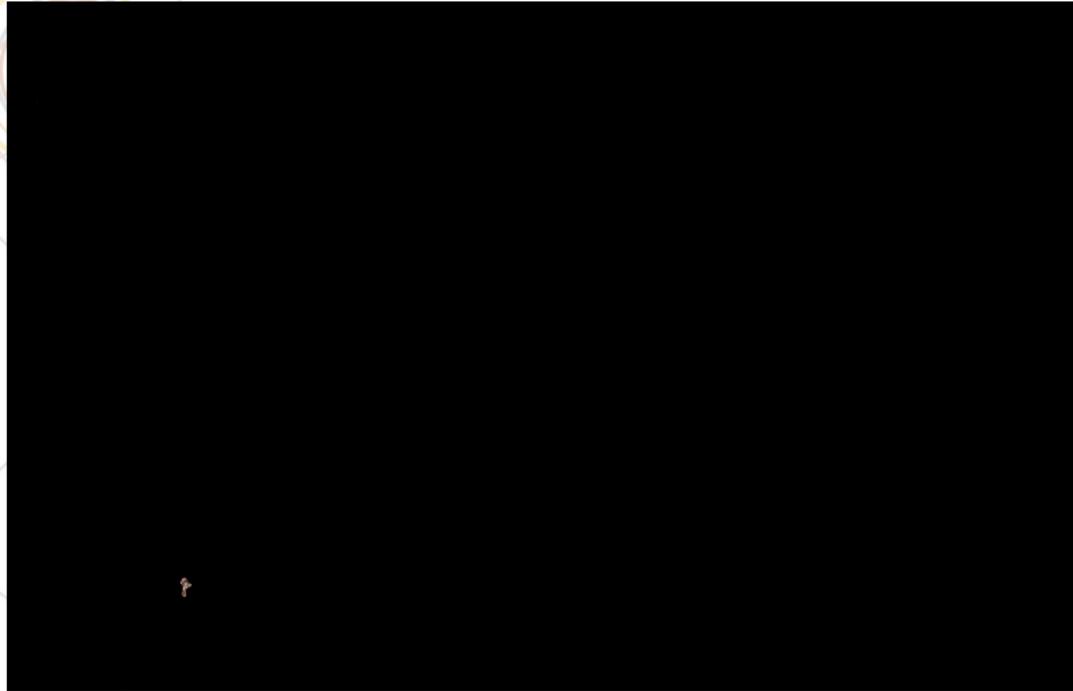




Introduction : zero-knowledge



Introduction : zero-knowledge



Introduction

Recommandations ANSSI



Agence nationale de la sécurité des systèmes d'information



EN CAS D'INCIDENT

ALERTES

PRESSE

RECRUTEMENT



UNE ADMINISTRATION



UNE ENTREPRISE



UN PARTICULIER

ACTUALITÉS

Recommandations pour une utilisation sécurisée de Zed!

Publié le 26 janvier 2016

La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques



Publié le 16 octobre 2015

#StratSecNum, suivez sur Twitter la présentation par Manuel Valls de la Stratégie nationale pour la sécurité du numérique.

« FIC 2016 : l'ANSSI agit pour la sécurité du numérique »

Publié le 22 janvier 2016

Agir pour la sécurité du numérique en France avec l'ANSSI - 100 postes à pourvoir d'ici 2017

Publié le 19 janvier 2016

Du nouveau pour les référentiels d'exigences applicables aux prestataires de cyberdéfense

Publié le 22 décembre 2015

Botconf 2015 : contrôler à distance un ordinateur totalement déconnecté du réseau, c'est possible !

Introduction

Recommandations ANSSI

Mécanismes cryptographiques - Règles et recommandations,
Rev. 1.20, ANSSI , 01/2010.

RègleCléSym-1. La taille minimale des clés symétriques utilisées jusqu'en 2020 est de 100 bits.

RègleCléSym-2. La taille minimale des clés symétriques devant être utilisées au-delà de 2020 est de 128 bits.

RecomCléSym-1. La taille minimale recommandée des clés symétriques est de 128 bits.

Introduction

Recommandations ANSSI



RègleAlgoBloc-1. Pour un algorithme de chiffrement ne devant pas être utilisé après 2020, aucune attaque nécessitant moins de $Nop = 2^{100}$ opérations de calcul doit être connue.

RègleAlgoBloc-2. Pour un algorithme de chiffrement utilisé au-delà de 2020, aucune attaque nécessitant moins de $Nop = 2^{128}$ opérations de calcul doit être connue.

RecomAlgoBloc-1. Il est recommandé d'employer des algorithmes de chiffrement par bloc largement éprouvés dans le milieu académique.

Introduction

Recommandations ANSSI



Factorisation

RègleFact-1. La taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020.

RègleFact-2. Pour une utilisation au-delà de 2020, la taille minimale du module est de 4096 bits.

RègleFact-3. Les exposants secrets doivent être de même taille que le module.

RègleFact-4. Pour les applications de chiffrement, les exposants publics doivent être strictement supérieurs à $2^{16} = 65536$.

Introduction

Recommandations ANSSI



RecomFact-1. Il est recommandé, pour toute application, d'employer des exposants publics strictement supérieurs à $2^{16} = 65536$.

RecomFact-2. Il est recommandé que les deux nombres premiers p et q constitutifs du module soient de même taille et choisis aléatoirement uniformément.

Introduction

La cryptologie n'est pas la stéganographie.



Introduction

La cryptologie n'est pas la **stéganographie**.



Je suis très émue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit là une 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 aussi vous dévoiler sans artifice mon âme toute nue, venez me faire une visite.

[...]

Introduction

La cryptologie n'est pas la **stéganographie**.



Je suis très émue de vous dire que j'ai
toujours une envie folle de me faire
baiser et je voudrais bien que ce soit
par vous. Je suis prête à vous montrer mon
cul, et si vous voulez me voir aussi
toute nue, venez me faire une visite.

[...]

Introduction

Quelques grandeurs

B. Schneier. Cryptographie appliquée.

Probabilité de mourir foudroyé (par jour)	1 chance sur 9 milliards (2^{33})
Probabilité de gagner le gros lot à la loterie américaine	1 chance sur 4 000 000 (2^{22})
Probabilité de gagner le gros lot à la loterie américaine et de mourir le même jour	1 chance sur 2^{61}
Probabilité d'être tué dans un accident automobile (aux États-Unis sur toute une vie)	1 chance sur 88 (2^7)
Âge de la Terre	10^9 années (2^{30})
Âge de l'Univers	10^{10} années (2^{34})
Nombre d'atomes constituant l'Univers	10^{77} (2^{265})

Un nombre de 1024 bit :

5858564308428828017644637396873011442410741924446401526444489392722401
2630691789482633773954538722685686046254635246206232275735158054157931
1060622915052999089708810050238601209069543816495749771173336617312655
2467966227874466635888109429506335487371428797711478405925439695590447
7668982192815149575434860493

Introduction

Quelques grandeurs

B. Schneier. Cryptographie appliquée.

Probabilité de mourir foudroyé (par jour)	1 chance sur 9 milliards (2^{33})
Probabilité de gagner le gros lot à la loterie américaine	1 chance sur 4 000 000 (2^{22})
Probabilité de gagner le gros lot à la loterie américaine et de mourir le même jour	1 chance sur 2^{61}
Probabilité d'être tué dans un accident automobile (aux États-Unis sur toute une vie)	1 chance sur 88 (2^7)
Âge de la Terre	10^9 années (2^{30})
Âge de l'Univers	10^{10} années (2^{34})
Nombre d'atomes constituant l'Univers	10^{77} (2^{265})

Un nombre de 1024 bit :

5858564308428828017644637396873011442410741924446401526444489392722401
2630691789482633773954538722685686046254635246206232275735158054157931
1060622915052999089708810050238601209069543816495749771173336617312655
2467966227874466635888109429506335487371428797711478405925439695590447
7668982192815149575434860493

(\sim 300 chiffres décimaux)

Introduction

Cryptologie :

▶ Cryptographie :

- ▶ conception de systèmes cryptographiques
- ▶ étude (preuve) de leur sécurité
- ▶ amélioration des performances

▶ Cryptanalyse :

- ▶ mise en défaut des systèmes cryptographiques
- ▶ attaque des problèmes algorithmiques sous-jacents
- ▶ observation des “canaux auxiliaires”

Introduction

Objectifs :

- ▶ **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime
- ▶ **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)
- ▶ **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- 
- ▶ **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime
 - ~~> chiffrement
 - ▶ **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)
 - ▶ **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- 
- ▶ **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime
 - ~~> chiffrement
 - ▶ **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)
 - ~~> identification/signature
 - ▶ **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

Introduction

Objectifs :

- ▶ **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime

~~> chiffrement

- ▶ **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier)

~~> identification/signature

- ▶ **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante

~~> hachage/signature

Introduction

Terminologie :

- ▶ Les acteurs : Alice, Bob, Charly, Ève
- ▶ (Message) clair m
- ▶ (Message) chiffré c
- ▶ Chiffrement : $c = E_{k_e}(m)$
- ▶ Déchiffrement : $m = D_{k_d}(c)$

$$D_{k_d}(E_{k_e}(m)) = m$$

Principes de Kerchoffs (La Cryptographie militaire – 1883)

Auguste Kerckhoffs von Nieuwenhof (19 janvier 1835 - 1903) est un cryptologue militaire néerlandais.

1. *Le système doit être matériellement, sinon mathématiquement indéchiffrable ;*
2. *Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;*
3. *La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;*
4. *Il faut qu'il soit applicable à la correspondance télégraphique ;*
5. *Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;*
6. *Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.*

L'âge artisanal

- ▶ IRAK XVIème avant JC :
potier → recette secrète sur une tablette d'argile : suppression des consonnes et modification de l'orthographe
- ▶ -600 : Nabuchodonosor (Babylone) tatouage sur le cuir chevelu



- ▶ VIIème avant JC : scytale
- ▶ Ier avant JC : chiffrement de César
- ▶ transposition, substitution (mono/poly-alphabétique, homophonique,...) - Vigénère,

L'âge technique

- ▶ machine à chiffrer (Enigma)
~~ automatisation

- ▶ naissance de l'informatique
~~ Turing, Colossus à Bletchley Park

- ▶ Data Encryption Standard
~~ du militaire au civil, prémisses de la théorie



L'âge paradoxal

- ▶ naissance de la
cryptographie à clé publique
on ne s'échange plus de clé : on la publie !

~~ chaque utilisateur possède un **couple**

$$(sk, pk)$$

où pk est publique et sk est gardée secrète

$$sk \xrightarrow{\mathcal{R}} pk$$

il est “*difficile*” de retrouver sk à partir de pk .

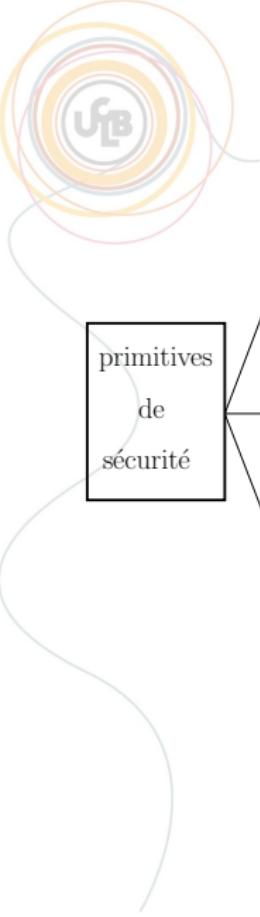


New Directions in Cryptography. W. Diffie and M. E. Hellman,
IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp 644–654.

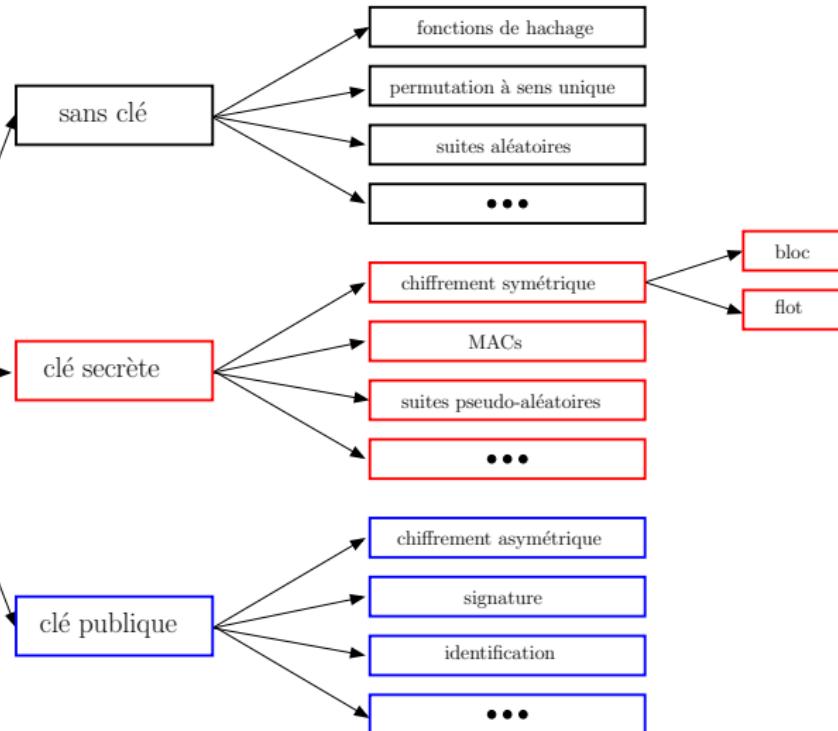


Dans tous les cas, un **secret**, partagé ou non, est nécessaire pour mettre en place un système cryptographique.

- ▶ cryptographie à clé secrète / cryptographie symétrique
clé secrète partagée
- ▶ cryptographie à clé publique / cryptographie asymétrique
clé secrète non divulguée



primitives
de
sécurité

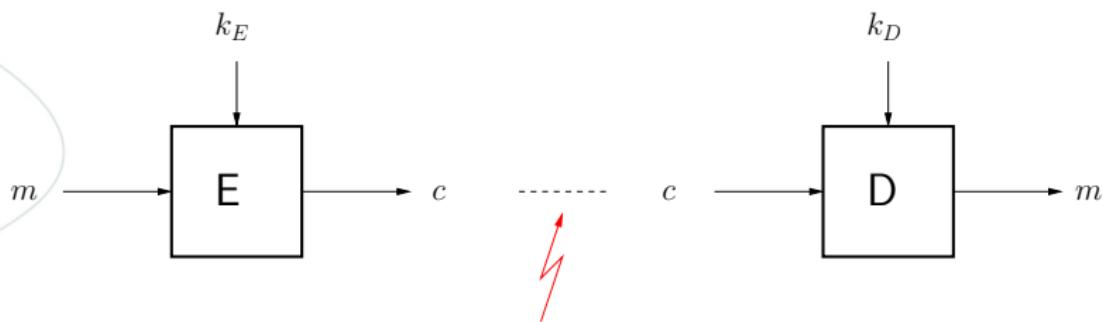


Confidentialité

Chiffrement



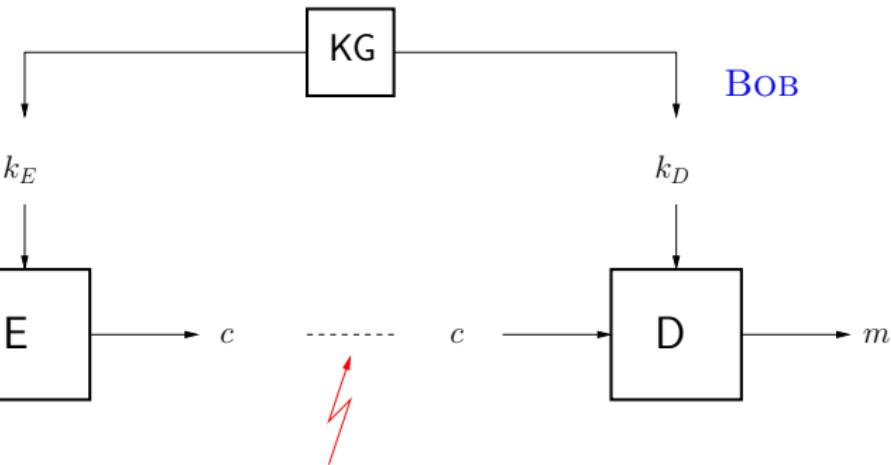
ALICE



- ▶ Encryption
- ▶ Decryption
- ▶ Key Generation

Confidentialité

Chiffrement



- ▶ Encryption
- ▶ Decryption
- ▶ Key Generation

Confidentialité

Chiffrement

Cryptographie à clé publique :

$$k_E \neq k_D \text{ et } \begin{cases} k_E = pk_{Bob} \\ k_D = sk_{Bob} \end{cases}$$

- ▶ Alice a obtenu la clé publique de Bob sur sa page web
- ▶ Bob et lui seul, grâce à sa clé secrète, peut déchiffrer

Remarque :

comment Alice est-elle sûre que la clé publique de Bob est bien la sienne ?

~~ certification des clés publiques par une autorité (ex. :  VeriSign)

Confidentialité

Chiffrement

Cryptographie à clé publique :

$$k_E \neq k_D \text{ et } \begin{cases} k_E = pk_{Bob} \\ k_D = sk_{Bob} \end{cases}$$

- ▶ Alice a obtenu la clé publique de Bob sur sa page web
- ▶ Bob et lui seul, grâce à sa clé secrète, peut déchiffrer

Remarque :

comment Alice est-elle sûre que la clé publique de Bob est bien la sienne ?

- ~~ certification des clés publiques par une autorité (ex. :  VeriSign)
- ~~ **Public Key Infrastructure** (enregistrement des utilisateurs, génération de certificats, renouvellement, révocation, séquestre...)

Confidentialité

Chiffrement

Les systèmes les plus « classiques » :

- ▶ RSA
- ▶ ElGamal
- ▶ NTRU
- ▶ McEliece

- ▶ Boneh-Franklin : chiffrement basé sur l'identité



Confidentialité

Chiffrement

Définition de la notion d'attaquant.

- ▶ Pour chaque systèmes cryptographiques :
 - ▶ ses **buts**
 - ▶ les **moyens** dont il dispose
- ▶ Attaques passives
 - ▶ Ève ne fait qu'observer la communication
- ▶ Attaques actives
 - ▶ Charly modifie le contenu des messages
 - ▶ destruction de messages
 - ▶ usurpation d'identité
 - ▶ déni de service
 - ▶ ...

Confidentialité

Chiffrement

Recherche exhaustive :

- ▶ on parcourt l'espace des clés
- ▶ Core 2 Quad (Penryn) - 3,2 GHz : $2 \times 24200 \text{ MIPS}^1$
 $1\,000\,000 \sim 2^{20}$
 2^{35} opérations en 1 seconde
- ▶ Recherche exhaustive sur 80 bits : $2^{80}/2^{35} = 2^{45}$ secondes
 $\leadsto 1114925$ années
- ▶ Recherche exhaustive sur 128 bits : $2^{128}/2^{35} = 2^{93}$ secondes
 $\sim 10^{27}$ secondes + 10^9 PC dans le monde en 2007
 $\leadsto 10^{18}$ secondes

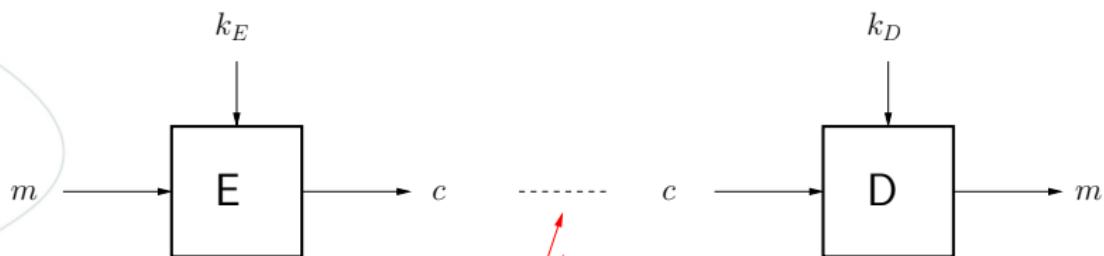
1. le nombre de millions d'instructions complétées par le microprocesseur en une seconde

Confidentialité

Chiffrement symétrique



ALICE



$$k_E = k_D$$

- ▶ Encryption
- ▶ Decryption
- ▶ Key Generation



Cryptographie à l'ancienne.

Substitution et Transposition

Substitution monoalphabétique

► substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- Chiffrement de César : permutation circulaire
 - $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé !

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow X

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow xq

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
 - ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow xqh

Substitution et Transposition

Substitution monoalphabétique

► substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

► Chiffrement de César : permutation circulaire

- $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
- $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

► décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow xqh k

Substitution et Transposition

Substitution monoalphabétique

► substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

► Chiffrement de César : permutation circulaire

- $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
- $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

► décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow xqh klurqghooh yroh gdqv oh flho

Substitution et Transposition

Substitution monoalphabétique

- ▶ substitution d'une lettre de l'alphabet du message en clair par une autre (du même ou d'un autre alphabet)

- ▶ Chiffrement de César : permutation circulaire

- ▶ $\mathbb{A} = \{a, b, c, d, e, \dots, x, y, z\} \leftrightarrow \{0, 1, 2, 3, 4, \dots, 23, 24, 25\}$
- ▶ $m = m_0m_1\dots m_n \rightsquigarrow E_3(m) = \pi_3(m_0)\pi_3(m_1)\dots\pi_3(m_n)$

$$\pi_3(i) = i + 3 \pmod{26}$$

- ▶ décalage de 3 lettres pas de clé!

Une hirondelle vole dans le ciel

\rightsquigarrow xqh klurqghooh yroh gdqv oh flho

- ▶ Permutation quelconque :

P	A	R	O	L	E	S
5	1	6	4	3	2	7
a	b	c	d	e	f	g
h	i	j	k	l	m	n
o	p	q	r	s	t	u
v	w	x	y	z		

La permutation :

a b c d e f g h i ...

b i p w f m t e l ...

Substitution et Transposition

Substitution monoalphabétique

- ▶ Si le nombre de lettres est 26, on a ?? clés possibles

Substitution et Transposition

Substitution monoalphabétique



Si le nombre de lettres est 26, on a **26!** clés possibles

$$26! \sim 2^{88}$$

Substitution et Transposition

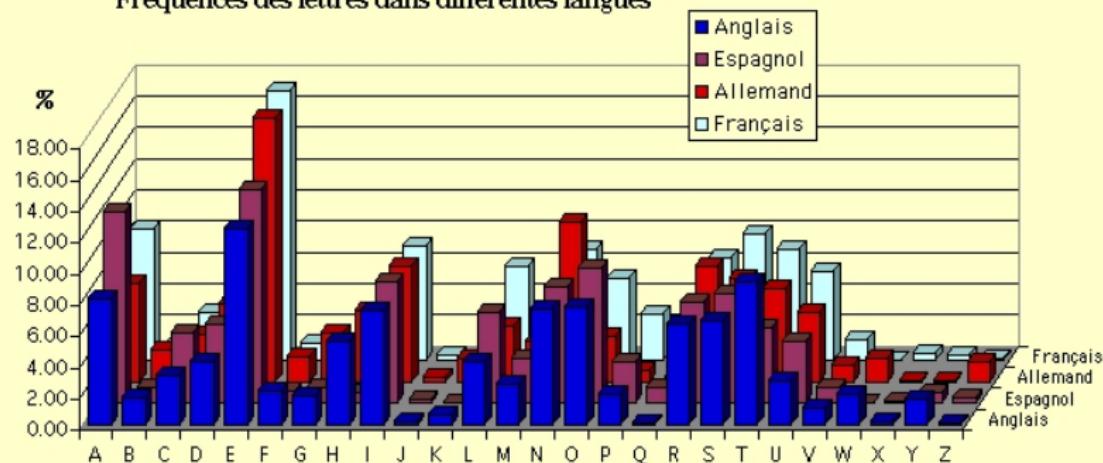
Substitution monoalphabétique

- ▶ Si le nombre de lettres est 26, on a **26!** clés possibles

$$26! \sim 2^{88}$$

- ▶ Ne cache pas la fréquence des lettres !

Fréquences des lettres dans différentes langues



Substitution et Transposition

Substitution monoalphabétique

Les bigrammes les plus fréquents (en nombre d'apparition sur 10 000 lettres)

es	305	te	163	ou	118	ec	100	eu	89	ep	82
le	246	se	155	ai	117	ti	98	ur	88	nd	80
en	242	et	143	em	113	ce	98	co	87	ns	79
de	215	el	141	it	112	ed	96	ar	86	pa	78
re	209	qu	134	me	104	ie	94	tr	86	us	76
nt	197	an	30	is	103	ra	92	ue	85	sa	75
on	164	ne	124	la	101	in	90	ta	85	ss	73
er	163										

Substitution et Transposition

Substitution monoalphabétique

On note

- ▶ ϕ_a la probabilité de présence de la lettre “a”
- ▶ β_{ab} la probabilité de présence du bigramme “ab”

On en déduit la probabilité de *transition* ω_{ab} qui est la probabilité de présence du bigramme “ab” sachant que “a” est la 1ère lettre du bigramme :

$$\omega_{ab} = \frac{\beta_{ab}}{\sum_x \beta_{ax}}$$

- ▶ Probabilité d'apparition du mot “chat” :

$$\Pr(\text{"chat"}) = \phi_c \phi_h \phi_a \phi_t = 0,0000017$$

Substitution et Transposition

Substitution monoalphabétique

On note

- ▶ ϕ_a la probabilité de présence de la lettre “a”
- ▶ β_{ab} la probabilité de présence du bigramme “ab”

On en déduit la probabilité de *transition* ω_{ab} qui est la probabilité de présence du bigramme “ab” sachant que “a” est la 1ère lettre du bigramme :

$$\omega_{ab} = \frac{\beta_{ab}}{\sum_x \beta_{ax}}$$

- ▶ Probabilité d'apparition du mot “chat” :

$$\Pr(\text{"chat"}) = \phi_c \phi_h \phi_a \phi_t = 0,0000017$$

- ▶ $= \Pr(\text{"ahct"})\dots$

Substitution et Transposition

Substitution monoalphabétique

De même

▶ $\Pr(\text{"qu"}) = 0,0007379 < \Pr(\text{"qe"}) = 0,00207\dots$

Substitution et Transposition

Substitution monoalphabétique

De même

- ▶ $\Pr(\text{"qu"}) = 0,0007379 < \Pr(\text{"qe"}) = 0,00207\dots$

Avec les probabilités de transition :

- ▶ $\Pr(\text{"chat"}) = 0,0000242$
- ▶ $\Pr(\text{"ahct"}) = 0,0000003$
- ▶ $\Pr(\text{"qu"}) = 0,01183$
- ▶ $\Pr(\text{"qe"}) = 0,0000$

Plus réaliste !

Substitution et Transposition

Substitution homophonique

- ▶ une lettre fréquente peut être remplacée par des signes différents

On “égalise” les fréquences :

- ▶ $a \leftrightarrow \{853, 514, 227, 702, 731\}$
- ▶ $b \leftrightarrow \{985\}$
- ▶ $c \leftrightarrow \{730, 611\}$
- ▶ $d \leftrightarrow \{467, 950\}$
- ▶ $e \leftrightarrow \{607, 339, 129, 616, 879, 803, 899, 290, 840, 726, 132\}$
- ▶ $f \leftrightarrow \{929\}$
- ▶ :

Nombre de symbole par lettre :

$$\max(1, \phi_x \cdot N \cdot C)$$

où N est le nombre de lettres du texte et C une constante

Substitution et Transposition

Substitution homophonique

- ▶ une lettre fréquente peut être remplacée par des signes différents

On “égalise” les fréquences :

- ▶ $a \leftrightarrow \{853, 514, 227, 702, 731\}$
- ▶ $b \leftrightarrow \{985\}$
- ▶ $c \leftrightarrow \{730, 611\}$
- ▶ $d \leftrightarrow \{467, 950\}$
- ▶ $e \leftrightarrow \{607, 339, 129, 616, 879, 803, 899, 290, 840, 726, 132\}$
- ▶ $f \leftrightarrow \{929\}$
- ▶ :

Nombre de symbole par lettre :

$$\max(1, \phi_x \cdot N \cdot C)$$

où N est le nombre de lettres du texte et C une constante

Cryptanalyse par King et Bahler

Substitution et Transposition

Substitution polyalphabétique

► substitution d'un symbole du clair par un autre qui dépend de l'état du cryptosystème

- plusieurs alphabets \Rightarrow même symbole chiffré différemment
- ex. : Vigenère (1586)

l	e	c	i	m	e	t	i	è	r	e	m	a	r	i	n
v	a	l	e	r	y	v	a	l	e	r	y	v	a	l	e

Cryptanalyse : déterminer la longueur de la clé \rightsquigarrow César

Substitution et Transposition

Substitution polyalphabétique

► substitution d'un symbole du clair par un autre qui dépend de l'état du cryptosystème

- plusieurs alphabets \Rightarrow même symbole chiffré différemment
- ex. : Vigenère (1586)

l	e	c	i	m	e	t	i	è	r	e	m	a	r	i	n
v	a	l	e	r	y	v	a	l	e	r	y	v	a	l	e
<hr/>															
g															

Cryptanalyse : déterminer la longueur de la clé \rightsquigarrow César

Substitution et Transposition

Substitution polyalphabétique

► substitution d'un symbole du clair par un autre qui dépend de l'état du cryptosystème

- plusieurs alphabets \Rightarrow même symbole chiffré différemment
- ex. : Vigenère (1586)

l	e	c	i	m	e	t	i	è	r	e	m	a	r	i	n
v	a	l	e	r	y	v	a	l	e	r	y	v	a	l	e
<hr/>															
g	e														

Cryptanalyse : déterminer la longueur de la clé \rightsquigarrow César

Substitution et Transposition

Substitution polyalphabétique

► substitution d'un symbole du clair par un autre qui dépend de l'état du cryptosystème

- plusieurs alphabets \Rightarrow même symbole chiffré différemment
- ex. : Vigenère (1586)

l	e	c	i	m	e	t	i	è	r	e	m	a	r	i	n
v	a	l	e	r	y	v	a	l	e	r	y	v	a	l	e
g	e		n												

Cryptanalyse : déterminer la longueur de la clé \rightsquigarrow César

Substitution et Transposition

Substitution polyalphabétique

► substitution d'un symbole du clair par un autre qui dépend de l'état du cryptosystème

- plusieurs alphabets \Rightarrow même symbole chiffré différemment
- ex. : Vigenère (1586)

l	e	c	i	m	e	t	i	è	r	e	m	a	r	i	n
v	a	l	e	r	y	v	a	l	e	r	y	v	a	l	e
g	e	n	m	d	c	n	i	p	v	v	k	v	r	t	r

Cryptanalyse : déterminer la longueur de la clé \rightsquigarrow César

Substitution et Transposition

Transposition

- ▶ caractères du texte inchangés ~ la position change
- ▶ Même fréquence dans le texte clair et son chiffré
- ▶ Ni vu ni connu ~ in uv in unnoc
- ▶ ex. : scytale

