La Cryptologie et le Vote

David Pointcheval

Ecole normale supérieure
Département d'Informatique
Équipe de Cryptographie

ENS
26 mars 2012

Plan

Plan

1. La Cryptologie
   - Histoire
   - Confidentialité
2. Vote

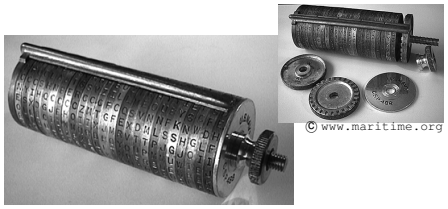
L'Âge Artisanal

Cryptologie = Science du Secret

**Historiquement,
but = confidentialité**

Scytale Lacédémonienne
Permutation

Disque d'Alberti
Substitution Mono-alphabetique

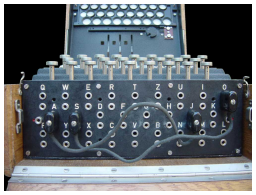


Cylindre – M 94 (CSP 488)
Substitution Poly-alphabetique

L'Âge Technique

Machines électro-mécaniques
(combinaisons de substitutions/permutations)
Paramétrisation par un secret commun: clé secrète

Enigma



Hagelin

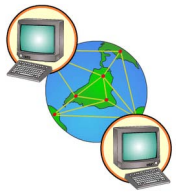
HAGELIN M-209 CIPHER MACHINE (GVG / PD)

L'Âge Moderne: Le Monde Numérique

Avec l'essor du tout-numérique, les besoins de sécurité se sont élargis: confidentialité, authentification, anonymat, ...

Au quotidien

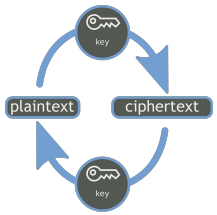
Travail/loisirs



Cryptographie Symétrique ou Asymétrique

Cryptographie Symétrique

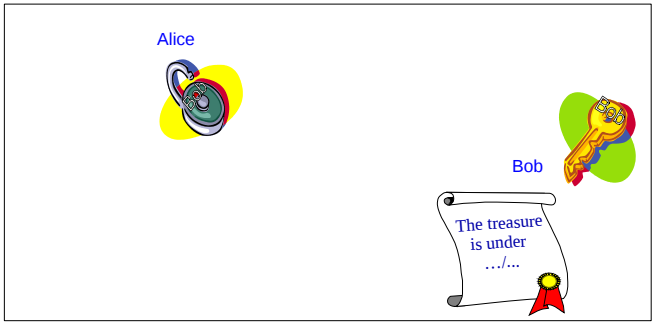
Une convention commune ou un paramétrage commun (clé secrète) sont partagés entre l'émetteur (Alice) et le destinataire (Bob)



**Le secret de cette clé
garantit la confidentialité
des communications**

La confidentialité nécessite-t-elle un secret pour l'émetteur ?

Cryptographie Asymétrique



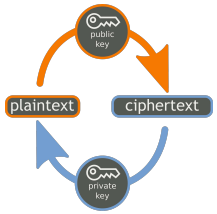
Chiffrement Asymétrique

- Un paramétrage public (la clé publique de Bob) permet à Alice de chiffrer un message à destination de Bob
- Un paramétrage secret (la clé secrète de Bob) permet à ce dernier de déchiffrer

Cryptographie Asymétrique

Chiffrement Asymétrique

- Un paramétrage public (la clé publique de Bob) permet à Alice de chiffrer un message à destination de Bob
- Un paramétrage secret (la clé secrète de Bob) permet à ce dernier de déchiffrer



Le secret de la clé secrète de Bob garantit la confidentialité des communications

Autres Fonctionnalités

La cryptographie peut apporter des solutions à de nombreux problèmes

- Confidentialité: Chiffrement
- Authentification: Signature, Protocoles d'identification
- Anonymat: signatures en blanc, signatures de groupe
- Preuves: preuves de calculs corrects, sur des données secrètes, sans révéler aucune information, autre que la validité des calculs
- etc

Plan

Choix des Desserts

Pour choisir un dessert, on met la liste suivante au vote

- ☐ Gâteau au chocolat
- ☐ Crème au caramel
- ☐ Glace à la vanille
- ☐ Fruit

Plusieurs types d'élections peuvent être effectués:

- Sélection d'un seul dessert: vote "uninominal" à 2 tours
- Sélection de plusieurs desserts: vote "plurinominal" à 2 tours

Vote préférentiel en 1 tour ?

Vote Préférentiel

- Chacun ordonne les propositions selon ses préférences
- Premiers choix: on élimine le perdant
- On fait remonter les choix suivants
- On recommence le décompte, etc

Gâteau au chocolat	1	1	3	2	3	3	3	1	3	
Crème au caramel	2	3	1	3	4	2	1	3	2	
Glace à la vanille	4	2	2	1	2	1	2	4	2	
Fruit	3	4	4	4	1	4	4	2	1	Éliminé
Gâteau au chocolat	1	1	3	2	2	3	3	1	3	
Crème au caramel	2	3	1	3	3	2	1	2	2	Éliminé
Glace à la vanille	3	2	2	1	1	1	2	3	3	
Gâteau au chocolat	1	1	2	2	2	2	2	1	3	
Glace à la vanille	2	2	1	1	1	1	1	2	5	Gagnant

Vote Préférentiel: Attaque de la Mafia

Si 12 candidats: près de 480 millions de séquences possibles
et près de 40 millions de séquences possibles avec un seul 1er choix
→ une séquence permet d'identifier un votant

Attaque de la Mafia

On va menacer les votants, en exigeant de voir apparaître telles séquences qui les identifiera:

- Votant 1: 5 - 3 - 9 - 1 - 10 - 2 - 8 - 7 - 4 - 11 - 6 - 12
- Votant 2: 5 - 1 - 12 - 3 - 10 - 6 - 8 - 7 - 4 - 11 - 2 - 9
- Votant 3: 5 - 12 - 3 - 7 - 2 - 10 - 8 - 1 - 4 - 11 - 6 - 9
- Votant 4: 5 - 1 - 9 - 12 - 3 - 2 - 8 - 4 - 7 - 11 - 6 - 10
- etc

→ les scrutins uninominaux ou plurinominaux sont préférés

Propriétés d'un Système de Vote

Liberté d'Expression

- Absence de contraintes extérieures

Sincérité

- Résultats conformes aux expressions des votants

Authentification

- Seules les personnes inscrites (votants) doivent pouvoir voter
- Les votants ne doivent pouvoir s'exprimer qu'une seule fois

Anonymat

- Votants et expressions des votes ne doivent pouvoir être reliés

Signature en Blanc

Signature en Blanc

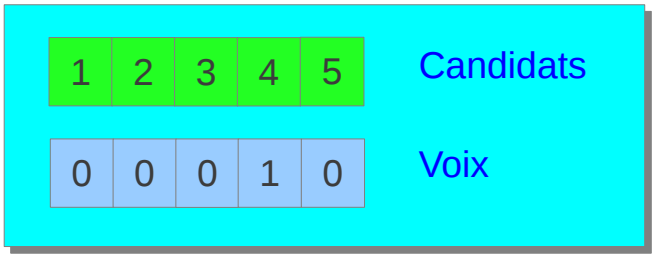
Le signataire signe un message sans le connaître,
ni même pouvoir le reconnaître ultérieurement

Vote à base de Signature en Blanc

- Chaque votant (après authentification / preuve d'appartenance à la liste électorale) fait signer son vote "en blanc"
  cela revient plus ou moins à retirer un sceau:
  unicité pour chaque votant
- Ensuite chaque votant va déposer (anonymement) son vote avec un sceau dans l'urne

Le problème technique réside dans le dépôt "anonyme":
on peut toujours identifier l'ordinateur émetteur

Vote: Bulletin de Vote



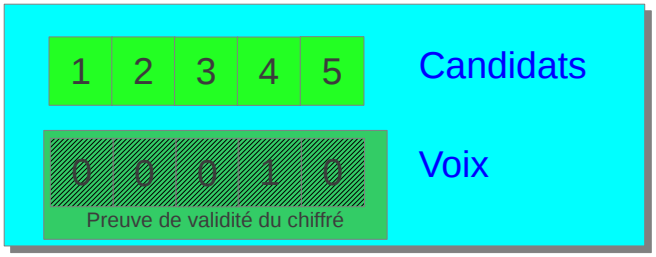
Le votant coche une seule case: mise à 1, les autres restent à 0
Scrutin: on additionne toutes les premières cases,
puis toutes les secondes cases, etc

58	32	109	88	12

Anonymat: Chiffrement Homomorphe

Pour garantir l'anonymat: les valeurs sont chiffrées
à destination du bureau de vote (chiffrement asymétrique)
Chiffrement homomorphe:
la somme des chiffrés est le chiffré de la somme
Déchiffrement distribué:
l'ensemble du bureau effectuera le déchiffrement du scrutin

Validité: Preuves



Chiffrement: masquage des valeurs
→ Fraude possible:

0	0	100	0	0
0	-99	100	0	0

Preuves de validité:
que des 0 et un seul 1 sont chiffrés

Authentification du Votant: Signature

Chiffrement: bulletin confidentiel
Authentification du votant: signature

Ce bulletin chiffré, prouvé, signé est déposé dans l'urne

Dépouillement

À l'issue du scrutin, avec le contenu de l'urne (qui peut être public), tout le monde peut

- vérifier l'authenticité des bulletins: signature
- vérifier l'unicité d'un bulletin par votant: une seule signature
- calculer la somme des chiffrés: chiffrement homomorphe
  $\rightarrow$ chiffrement du scrutin final

L'ensemble du bureau déchiffre le chiffré: scrutin final

- déchiffrement distribué: confidentialité des bulletins
- déchiffrement vérifiable: sincérité du scrutin

Tout est publiquement vérifiable: vérifiabilité universelle

Comparaison avec le Vote Traditionnel

- Authenticité/unicité: émargement
  (*signature = émargement*)
- Anonymat/confidentialité: enveloppe
  (*chiffrement = enveloppe*)
- Sincérité du scrutin: urne transparente, ...
  et présence dans tous les bureaux de vote
  (*vérifiabilité de toutes les étapes, même a posteriori*)
- Liberté d'expression: bureau de vote, isoloir, pas d'annotation
  $\rightarrow$ on peut forcer un vote nul!
  (en imposant une annotation)

Vote électronique, par internet $\neq$ "depuis n'importe où"
e.g., dans tout bureau de vote: local approprié (isoloir)
Si risque de vote sous contrainte: possibilité de voter plusieurs fois, seul le dernier vote compte: possible avec l'heure d'émargement

Contestations Usuelles contre le Vote Électronique

- Si attaque, attaque massive
  - Aucune raison d'avoir un unique serveur centralisé
  - Résultats par bureaux de vote
  - L'important est la sincérité du vote
    en cas d'attaque ou de faille, on recommence
- Anonymat: attaques Tempest (émissions électro-magnétiques) qui permettent de lire un clavier/écran à distance
  - Méthodes très sophistiquées/coûteuses
  - Vote classique: empreintes digitales sur un bulletin
- Vérifiabilité complexe, alors qu'avec le vote classique, une urne et des enveloppes, c'est simple pour tous
  - Une personne ne peut vérifier tous les bureaux de vote
  - Or, la vérifiabilité universelle permet toute vérification, a posteriori
    mais demande une expertise

Conclusion

La cryptographie permet d'apporter l'analogue numérique à de très nombreux outils classiques

- Enveloppe: Chiffrement
- Emargement: Signature

Elle permet même des choses inattendues

- Calculs sur des données chiffrées
- Preuves convaincantes sans rien révéler de superflu

$\rightarrow$ analogue électronique à une élection

Les principaux problèmes sont dans l'initialisation du système:

- la constitution de la liste électorale (source de contestations)
- l'authentification du votant (source de fraudes)

Ces problèmes se retrouvent dans tous les systèmes de vote classiques et électroniques