Pour la libéralisation de la cryptographie

AUBERT Jérôme
ROUSSE David
DESS MIAGe

Plan

I. Introduction

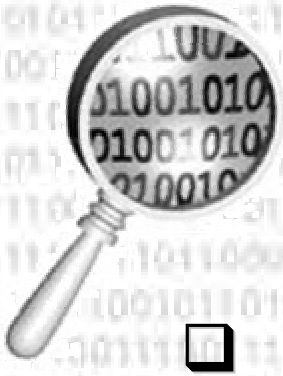
II. Préambule sur la sécurité des communications

III. A l'origine, la cryptographie vue comme une arme

IV. Utilisation de la cryptographie, antagonisme des besoins privés face à la raison d'état

V. Les évolutions nécessaires pour la protection de la vie privée

VI. Conclusion et discussion

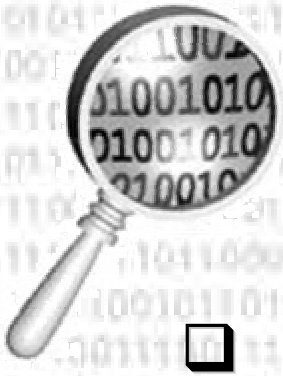


Introduction

- **Information**
  matière première immatérielle primordiale dans la société actuelle

- **Historique**
  besoin de masquer l'information apparu très tôt
  complexification progressive du chiffrement
  science mathématique à part entière enfin

- **Définition**
  transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de convention

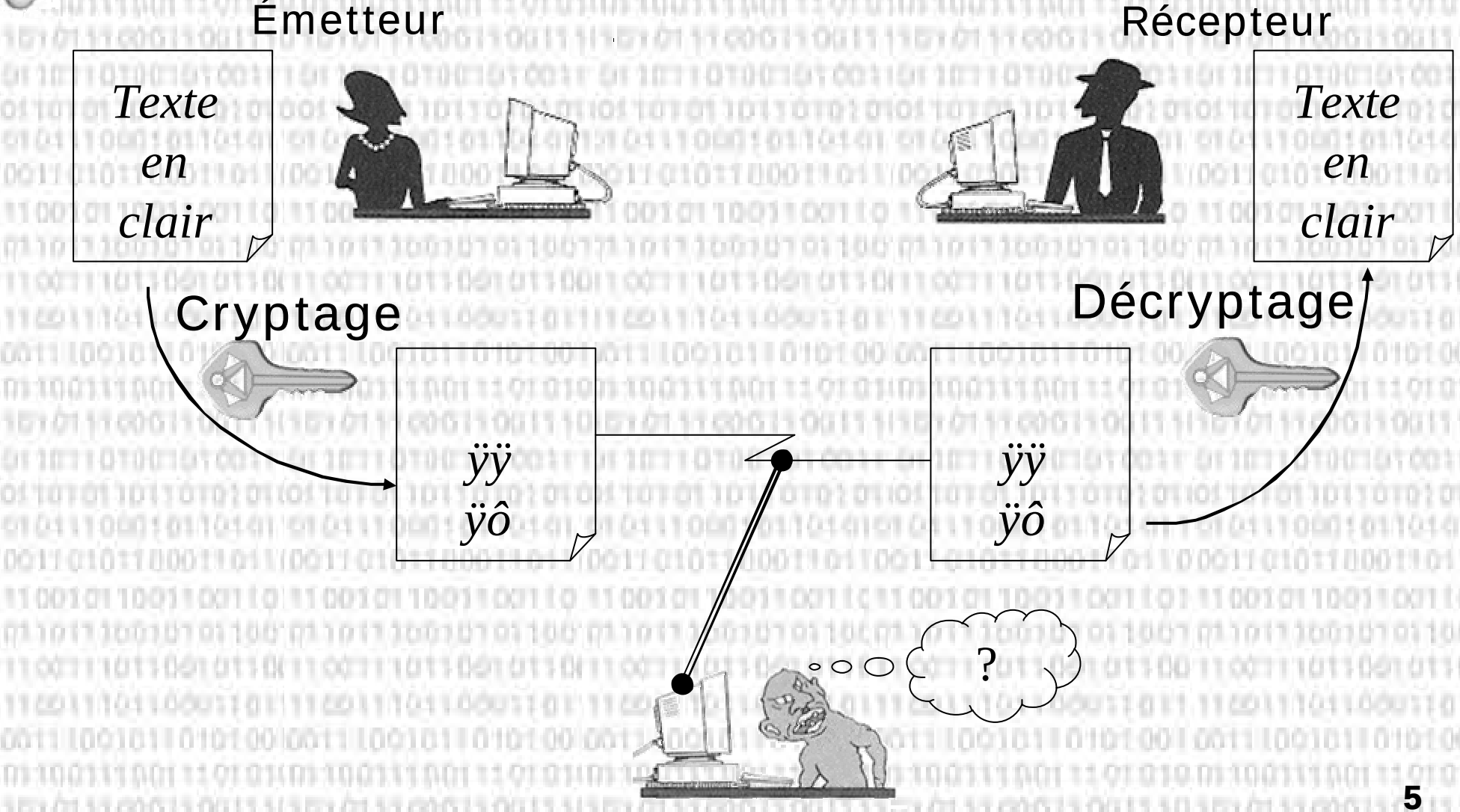


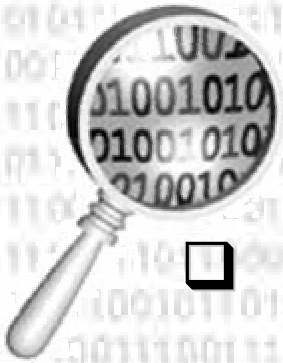
Préambule sur la sécurité des communications

- **Confidentialité**
  maintien secret de l'information, accessible seulement aux entités autorisées
- **Intégrité**
  message intègre et non altéré
- **Authentification**
  assurance de l'identité de l'interlocuteur
- **Non-répudiation**
  aucune contestation possible quand à l'identité de l'émetteur

Principe cryptographique

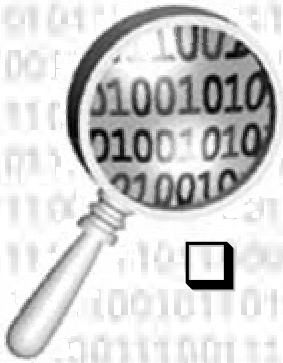
❑ Utilisation de clé de cryptage





Cryptographie à clé secrète

- **Chiffre de César**
  messages cryptés par substitution, envoyés à ses légions
- **Méthode de Vigenère**
  combinaisons de substitutions
- **Cryptogramme de Polybe**
  élimine les relations statistiques entre texte chiffré et texte clair
- **DES**
  méthode de cryptage, forte en 1970, ne l'est plus aujourd'hui
- **AES et Rijandel**
  évolutions de DES
- **La distribution des clés secrètes est problématique**



Cryptographie à clé publique

- **Système Diffie – Hellman - Merkle**
  facilite la distribution des clés secrètes via un système de chiffrement asymétrique
- **RSA**
  conçu (à partir des travaux de DHM) au MIT par Rivest, Shamir et Adleman
  assure confidentialité, intégrité, authentification et non-répudiation
- **Distribution des clés publiques**
  tiers de confiance (autorités de certification)
  certificats numériques (X.509)
- **Signature numérique**
- **Enveloppe digitale**

A l'origine, la cryptographie vue comme une arme

- **La raison d'État avant tout …**

1- La cryptographie doit faire l'objet d'un cadre juridique

2- La législation française à ses débuts

3- La législation dans d'autres pays : UE et USA

Antagonisme des besoins privés face à la raison d'état

- **Comment réussir à protéger des intérêts souvent divergents ?**

1- Protection de l'État
   a- contre des interventions « extérieures »
   b- contre des interventions à l'intérieur même des sociétés

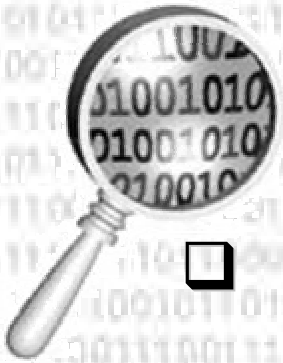
2- Protection de l'individu
   a- la vie privée
   b- la privacy

Les évolutions nécessaires pour la protection de la vie privée

- **La tendance pour le futur semble être à la libéralisation, mais …**

1- Des initiatives de l'État qui tendent vers une généralisation de la pratique de la cryptographie

2- A l'heure de la globalisation, les individus ressentent le besoin d'un échange facile et sûr d'information



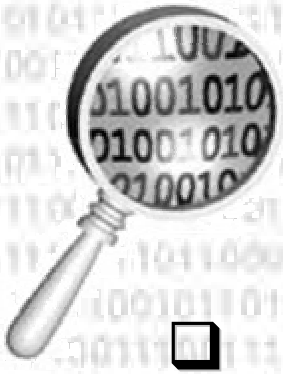
L'exemple de PGP

- **PGP (Pretty Good Privacy)**
  créé par Phil Zimmermann :

  « les références de l'État américain n'incitent guère à penser qu'il n'abusera jamais de nos libertés civiles »

- **Principe**
  PGP n'emploie pas de CA
  chaque utilisateur gère ses propres certificats
  plusieurs personnes signent un même certificat
  clé publique validée au final par empreinte

  système de confiance mutuelle



Conclusion - Discussion

- **Utilisation des tiers de confiance**
  infrastructures basées sur des tiers de confiance … contrôlées par l'État

- **Utilisation totalement libéralisée**
  grâce à travaux comme ceux de Zimmermann, il devient possible de choisir comment gérer la sécurité de nos communications

AUBERT Jérôme
ROUSSE David