



# Comment chiffrer ses emails?

Benjamin Bouvier  
Balthazar Rouberol





# Le chiffrement : pourquoi faire ?

Faire transiter des informations sur un média potentiellement compromis, seulement lisible par l'expéditeur et le destinataire.

- Email
- Fichiers
- Texte
- etc

# Pourquoi chiffrer ?



# Pourquoi ça marche ?

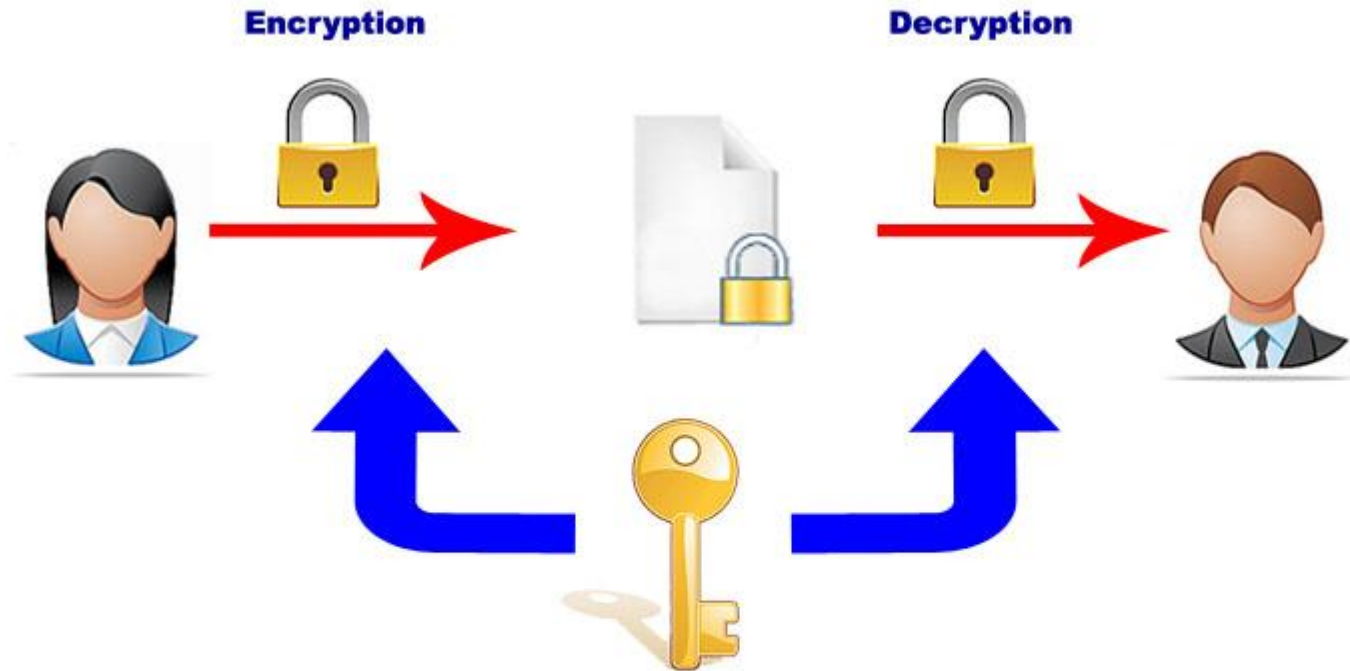
$p, q$

$$n = pq \quad \phi(n) = (p - 1)(q - 1)$$

$$e, \quad 1 < e < \phi(n) \quad \gcd(e, \phi(n)) = 1$$

$$d = e^{-1} \text{ mod } \phi(n)$$

# Chiffrement symétrique

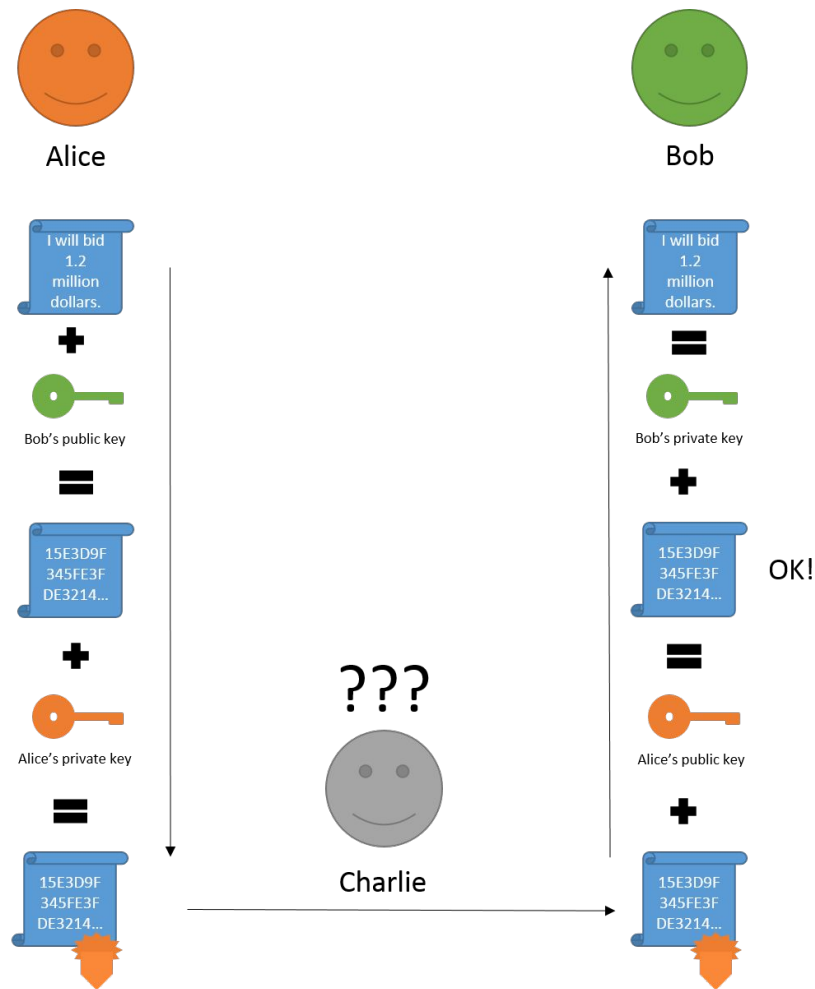






# Chiffrement asymétrique

- **Chiffrement** : cacher le contenu du message
- **Signature** : prouver l'identité de l'expéditeur
  
- **Clé publique** : distribuable à tout le monde
- **Clé privée** : ne doit PAS être distribuée

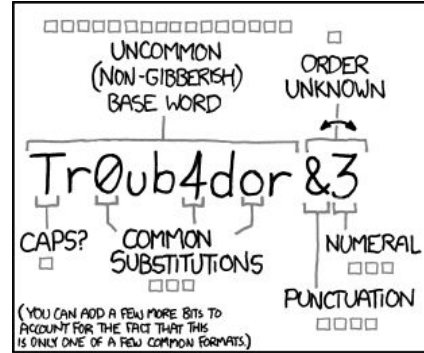




# Comment choisir une bonne *passphrase* ?

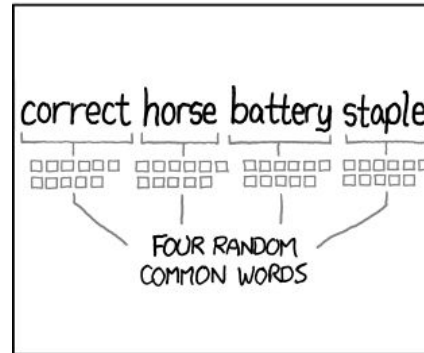
## Diceware

<https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>





~28 BITS OF ENTROPY  
□□□□□□□□ □  
□□□□□□□□ □  
□□□ □□□  
 $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$   
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)  
DIFFICULTY TO GUESS:  
**EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?  
AND THERE WAS SOME SYMBOL...   
DIFFICULTY TO REMEMBER:  
**HARD**



~44 BITS OF ENTROPY  
□□□□□□□□□□  
□□□□□□□□□□  
□□□□□□□□□□  
□□□□□□□□□□  
 $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$   
DIFFICULTY TO GUESS:  
**HARD**

THAT'S A BATTERY STAPLE.   
CORRECT!   
DIFFICULTY TO REMEMBER:  
YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Comment distribuer sa clé publique?

- Envoi par mail
- En main propre
- Sur votre site personnel
- Sur des keyservers (serveurs de distribution de clés publiques)
- [Keybase.io](https://keybase.io)

# Réseau de confiance

- Comment peut-on faire confiance à une clé trouvée sur internet? En regardant à qui d'autres à qui on fait confiance ont déjà fait confiance.
- [Keybase.io](https://keybase.io) lie une cle à une identité numérique

# Limites du chiffrement

- Métadonnées: seul le contenu du mail est chiffré, pas les metadonnées (expéditeur, destinataire, IP de provenance, client mail utilisé, etc.)
- Difficulté d'utilisation sur plusieurs appareils
- Investissement initial (apprentissage, expérience utilisateur)

# Outils

- GPG
- Thunderbird + Enigmail
- Evolution
- Mail.app + GPGTools
- Mailvelope