Comment chiffrer ses emails?

Benjamin Bouvier
Balthazar Rouberol


public class PrimitiveParameters
{
public static void main(String[] args)
{go();
}
public static void go()
{int x = 3;
int y = 2;
System.out.println("In method go. x: " + x + " y: " + y);
falseSwap(x,y);
System.out.println("in method go. x: " + x + " y: " + y);
moreParameters(x,y);
System.out.println("in method go. x: " + x + " y: " + y);
}
public static void falseSwap(int x, int y)
{System.out.println("in method falseSwap. x: " + x + " y: " + y);
int temp = x;
x = y;
y = temp;
System.out.println("in method falseSwap. x: " + x + " y: " + y);
}
public static void moreParameters(int a, int b)
{System.out.println("in method moreParameters. a: " + a + " b: " + b);
a = a * b;
System.out.println("in method moreParameters. a: " + a + " b: " + b);
}

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 ?

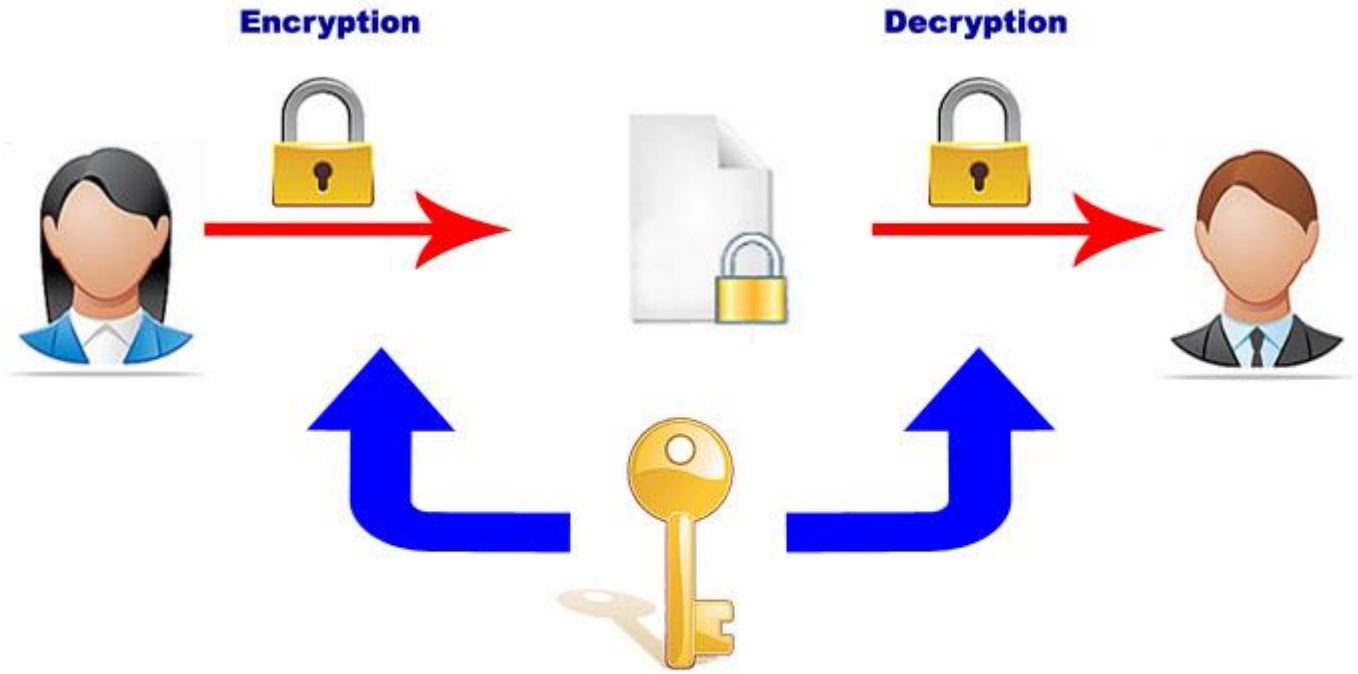
$$p, q$$

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

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

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

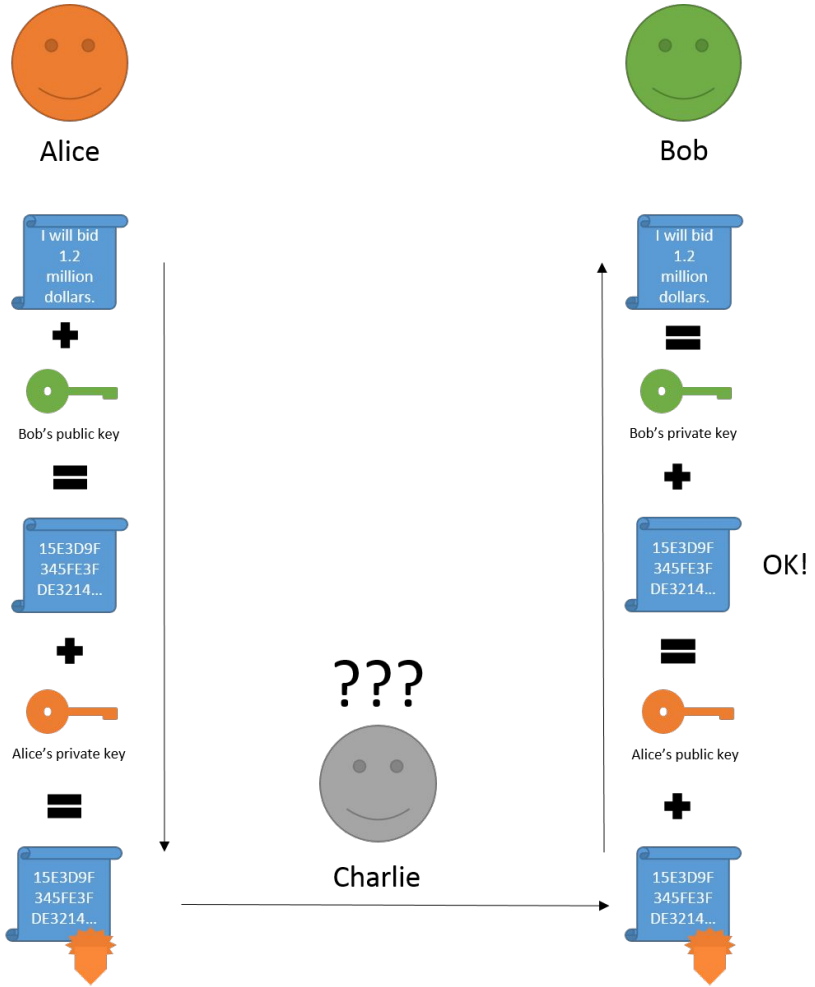
Chiffrement symétrique



Chiffrement asymétrique

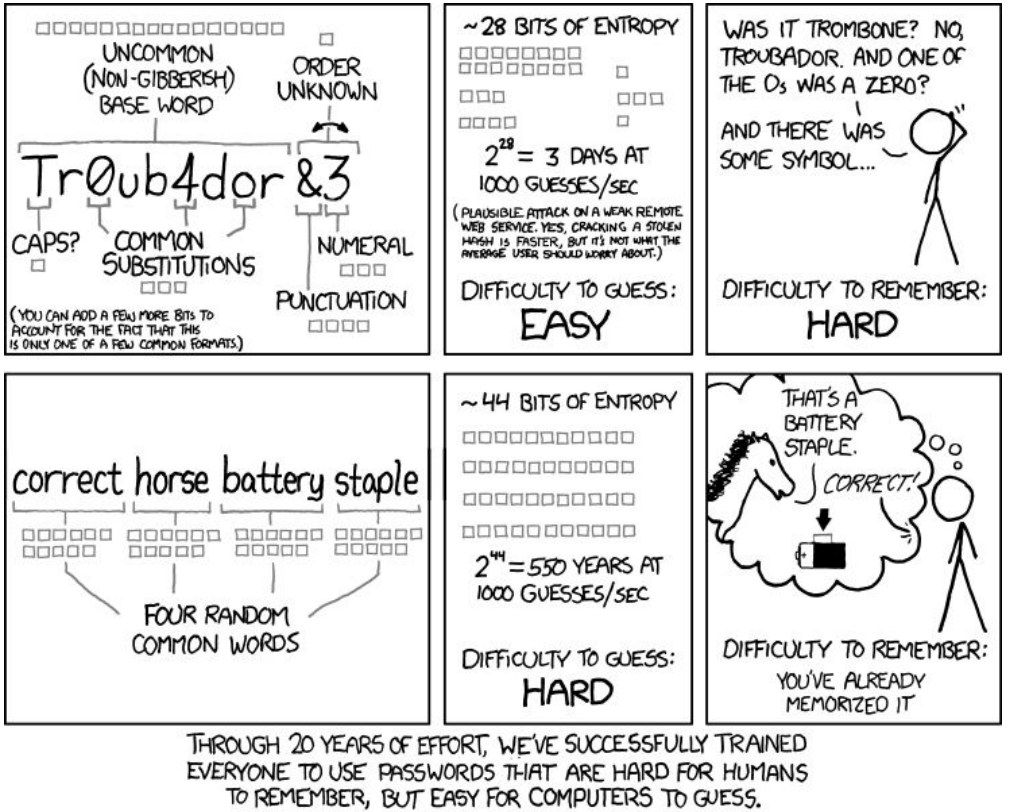
- **Chiffrement** : cacher le contenu du message
- **Signature** : prouver l'identité de l'expéditeur

- **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/



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

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 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