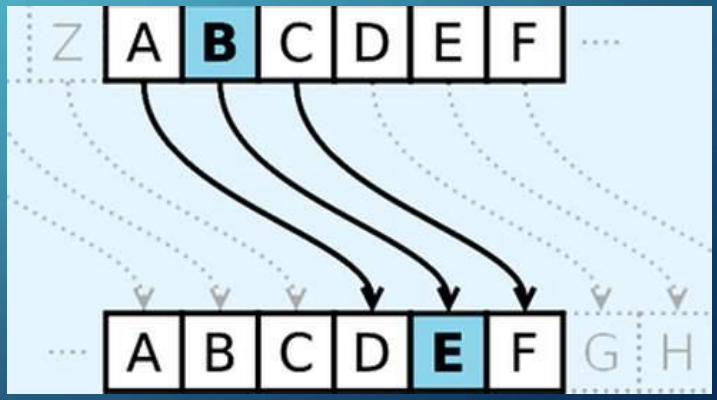
DE LA KRYPTO(NITE)… ET DU GENRE 2

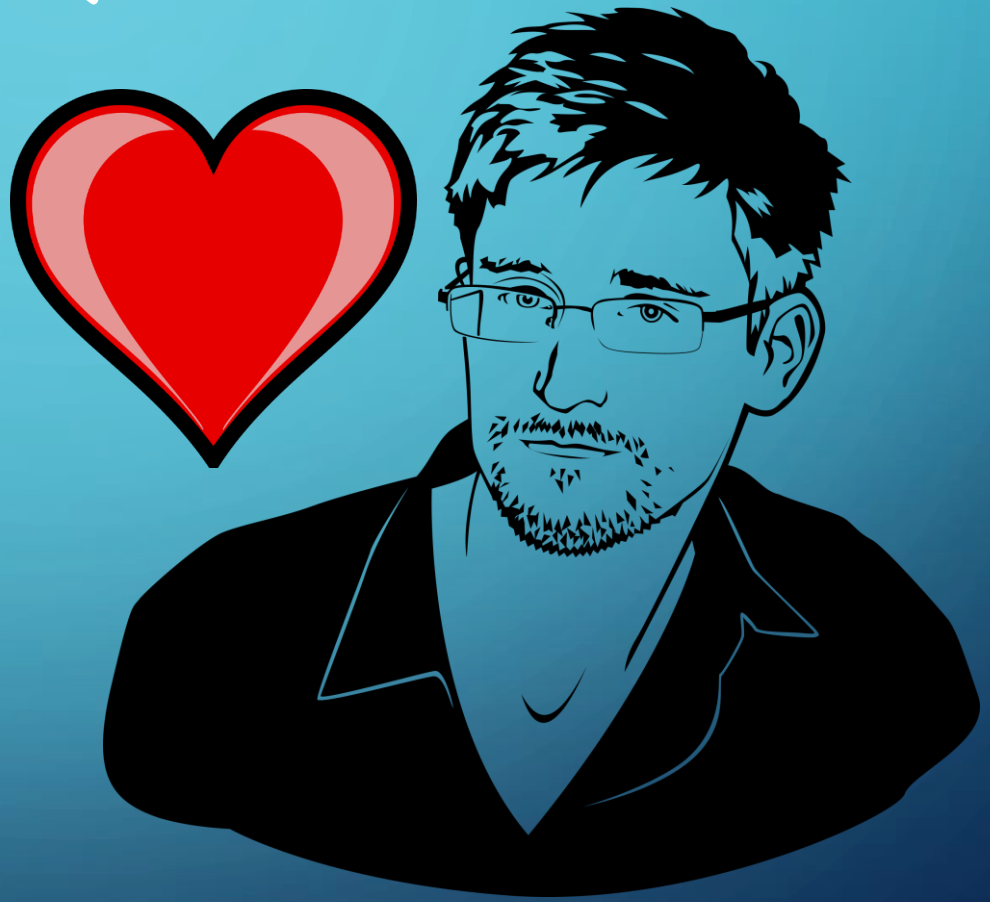
N. Du Hamel

LA CRYPTO

La science et l'art de transformer des messages pour les rendre sécurisés et insensible aux attaques



POURQUOI ?

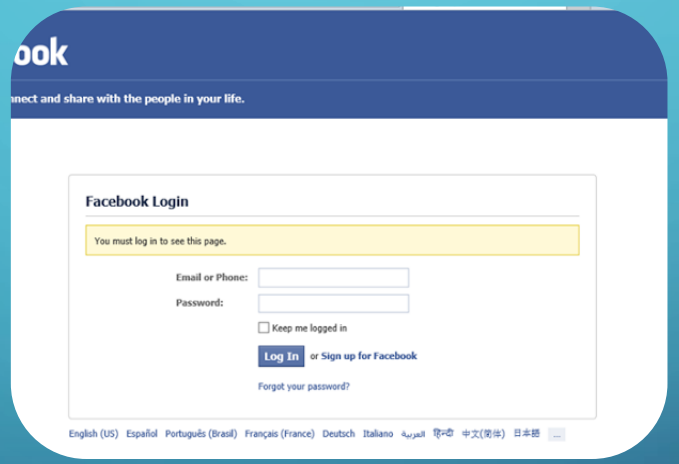


Prism, Angry birds, The Smurfs…

Citizenfour

PROBLÉMATIQUES

Confidentialité

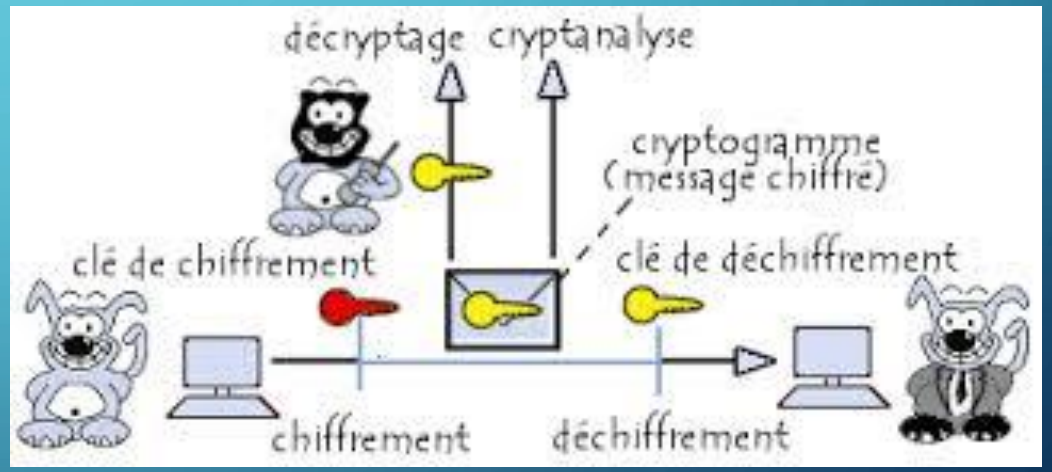


Authentification

Intégrité

CONFIDENTIALITÉ

La **confidentialité** est définie comme « le fait de s'assurer que l'information n'est seulement compréhensible qu'à ceux dont l'accès est autorisé ».



VIE PRIVÉE ET GOOGLE

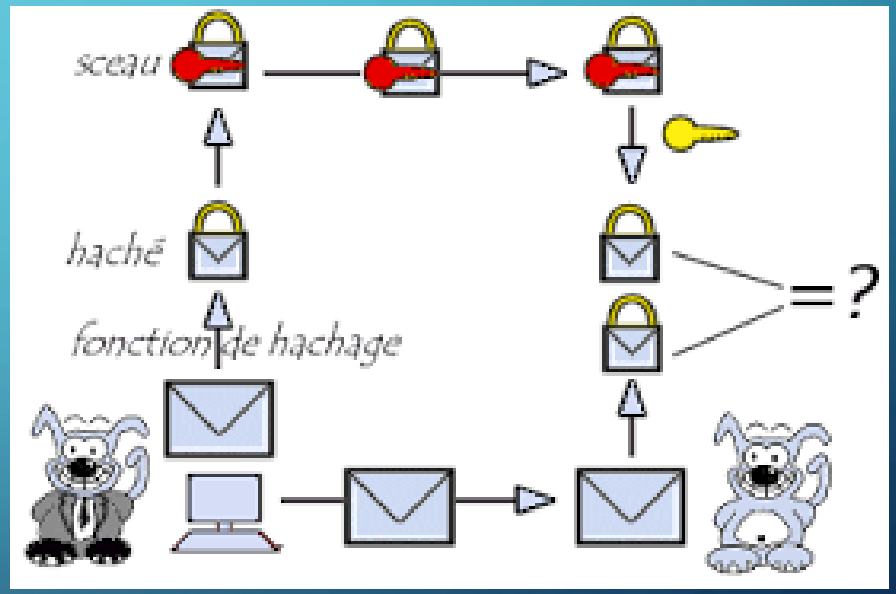
« Les personnes qui envoient un mail à l'un des 425 millions d'utilisateurs de Gmail n'espèrent pas que leur message reste confidentiel »

AUTHENTIFICATION

L'**authentification** est la procédure qui consiste à vérifier l'identité d'une personne afin de lui autoriser l'accès à certaines ressources.

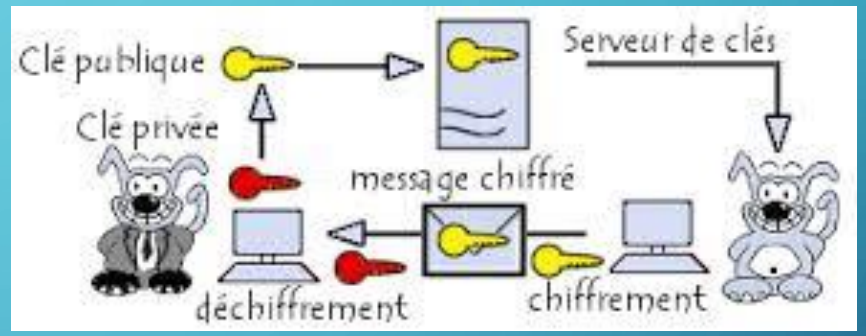
INTÉGRITÉ

L'intégrité est la procédure qui consiste à vérifier qu'il n'y a pas eu de falsification des données et à s'assurer que l'émetteur est bien celui que l'on croit.



CRYPTO SYMÉTRIQUE/ASYMÉTRIQUE

- On utilise la même clé pour le chiffrement/déchiffrement
- La clé doit être gardée secrète
- Alice et Bob doivent partager un secret commun



- Une clé pour le chiffrement et une autre pour le déchiffrement
- Une des deux clés doit être gardée secrète
- Alice et Bob n'ont pas besoin d'un secret commun

ÉCHANGE DE CLÉS

Eve

Alice

Bob

ÉCHANGE DE CLÉS

Eve

Alice

Bob

ÉCHANGE DE CLÉS

Eve

Alice

Bob

Private

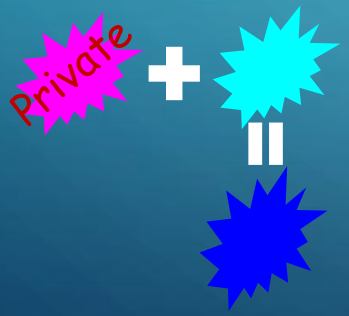
Private

ÉCHANGE DE CLÉS

Eve

Alice

Bob

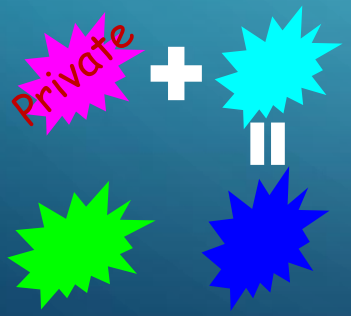


ÉCHANGE DE CLÉS

Eve

Alice

Bob



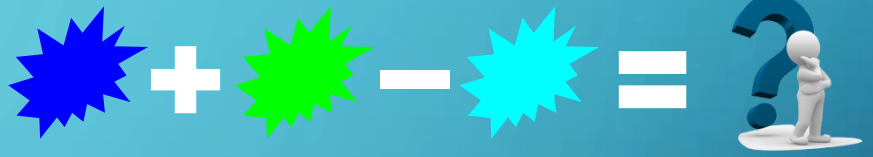
ÉCHANGE DE CLÉS

Eve

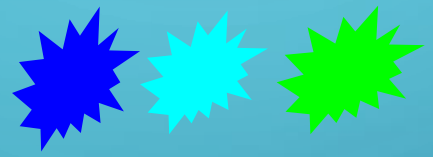
Alice

Bob

ÉCHANGE DE CLÉS



Eve



Alice

Bob

DES MATHS….

- Alice et Bob choisissent publiquement un groupe cyclique G et un générateur P
- Alice choisit un entier a (privé) et envoie aP à Bob
- Bob choisit un entier b (privé) et envoie bP à Alice
- Alice calcule $a(bP)=abP$
- Bob calcule $b(aP)=abP$

DU *GENRE 2*

Une *courbe de genre 2* est une courbe algébrique définie par une équation de la forme

$$y^2 = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + f_6 x^6$$

où le polynôme de degré 6 est à racines simples dans la clôture algébrique.

/* CARAMEL */

```
    d[5],Q[999                ]={0};main(N                C,A,
  (;i--;e=scanf("%"          "d",d+i));for(A             R,a,
 ++i<A          ;++Q[      i*i%          A],R=         M,E,
R:i);             for(;i  --;)           for(M       L,i=
--;N              +=!M*Q [E%A            ],e+=      5,e,
+E*E-            R*L*    L%A)           %A])      ){for
  E=i,L=M,a=4;a;C=          i*E+R*M*L,L=(M*E      =*d;
    %A,E=C%A+a               --[d]);printf       i[Q]?
                                                 =A;M
                                                 Q[(A
                                                  for(
                                                  +i*L)
                                                   ("%d"
                                                    "\n",
                                                     (e+N*
                                                       N)/2
                                                        -A);}
/* cc caramel.c; echo f3 f2 f1 f0 p | ./a.out */
```

FAST GENUS 2 ARITHMETIC BASED ON THETA FUNCTIONS

Théorème (Gaudry). *Soit P un point sur la surface de Kummer dont les coordonnées sont non nulles et $n > 1$ un entier. Le calcul de nP nécessite $16 \log_2 n$ produits et $9 \log_2 n$ élévations aux carrés.*

Amélioration des constantes par rapport au genre 1

STAGE : CALCUL DE $\sqrt{2}$

- On se restreint à un sous-groupe cyclique $\mathrm{G} \cong Z/nZ$
- L'endomorphisme agit comme une multiplication par $\sqrt{2}$
- On veut effectuer une multiplication scalaire par m
- On écrit $\mathrm{m} = a + b\sqrt{2}$, où les entiers a et b sont de l'ordre de $\sqrt{n}$
- On calcule notre multiplication scalaire $\mathrm{m}P = aP + b(\sqrt{2}P)$

LA THÈSE…

Proposition. *Avec les formules thêtas de [Gaudry, 2007], le calcul d'une multiplication scalaire d'un point P sur la surface de Kummer par un entier $n > 1$ nécessite $11{,}5 \log_2 n$ produits, $6{,}5 \log_2 n$ élévations au carré dans le corps de base et le calcul de $(1 + \sqrt{2})P$.*

Et pourquoi pas du comptage de points ou même du log discret…

REMERCIEMENTS

Merci à Alice, Ben et
François, Rafik et
pour finir vous tous…