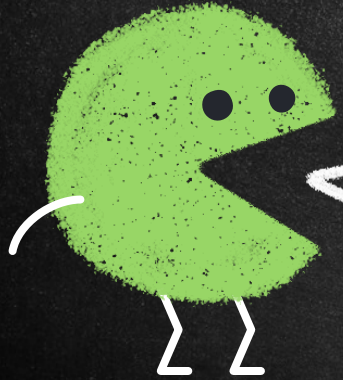
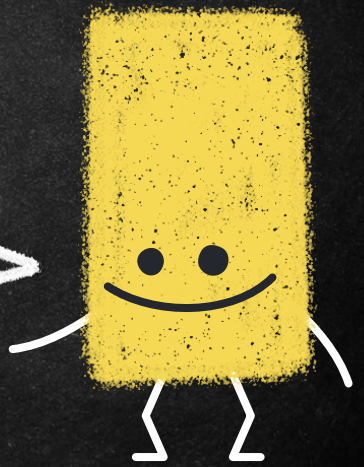
Sécurité des données
A2021

Encryption Asymétrique

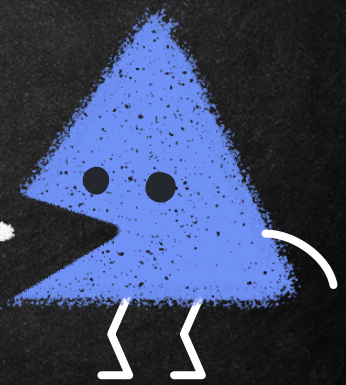




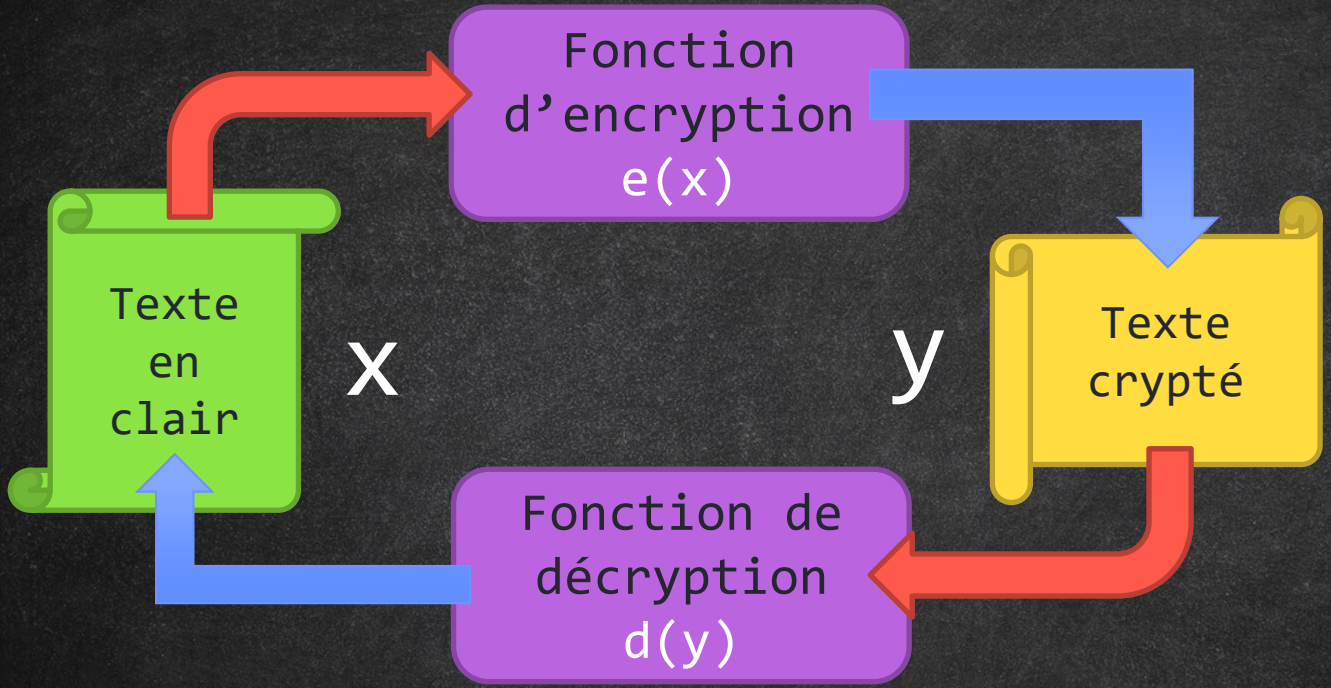
Yannick Charron

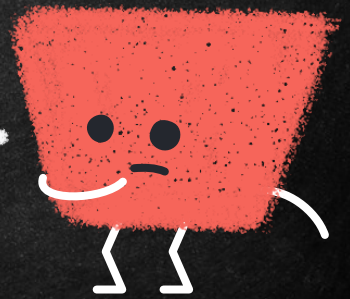
Plan de la séance

- Concept général
- Clé privée et clé publique
- RSA
- Signature
- Applications



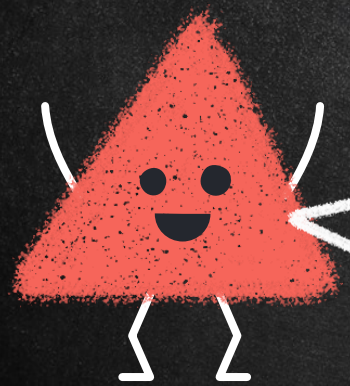
Concept Général

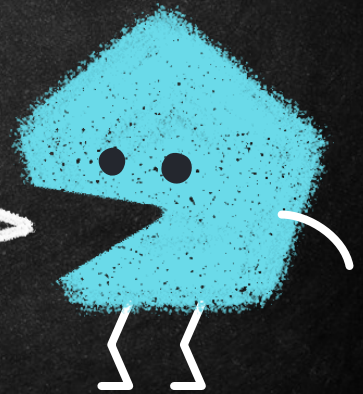


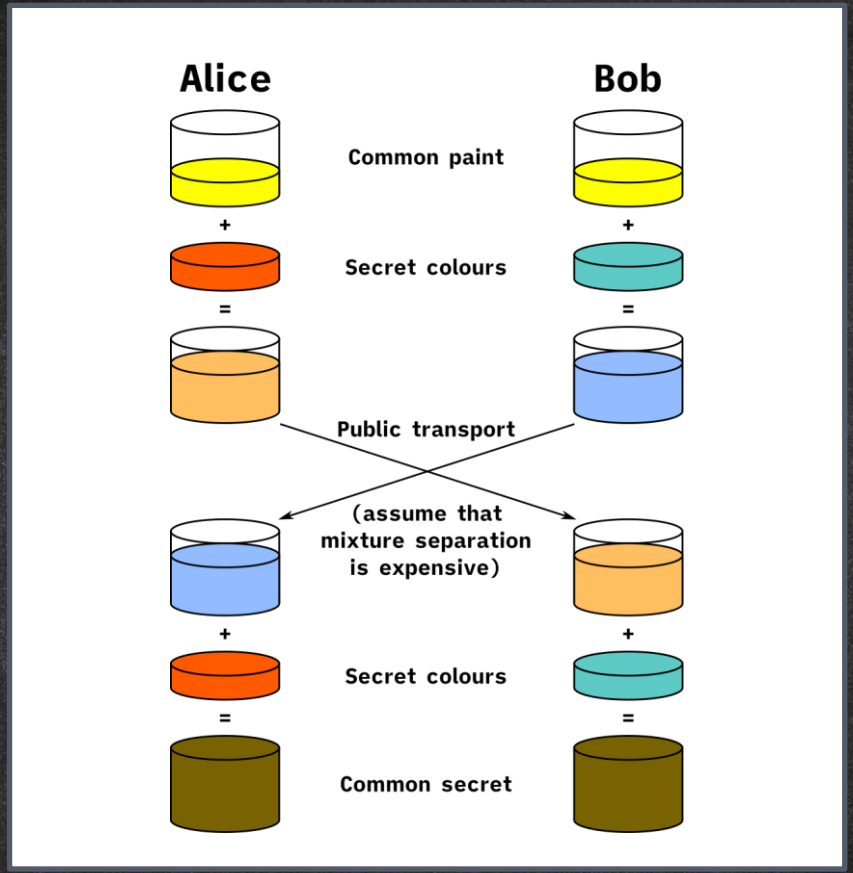


Diffie-helleman

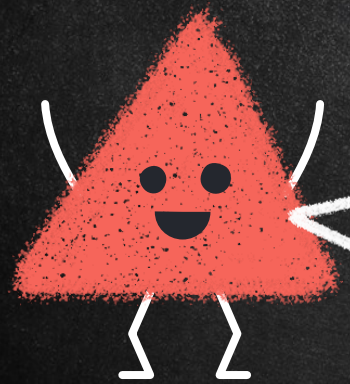
Échange d'une clé

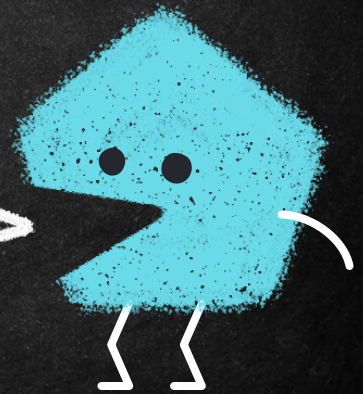





Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume that
mixture separation
is expensive)
+
Secret colours
=
Common secret

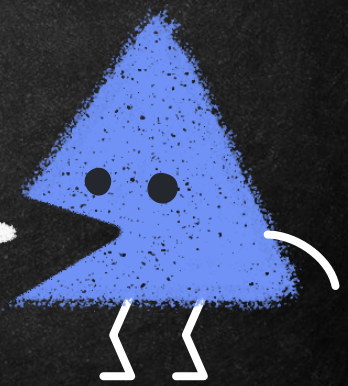
Un peu de mathématiques



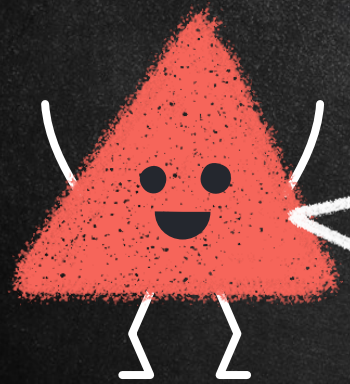


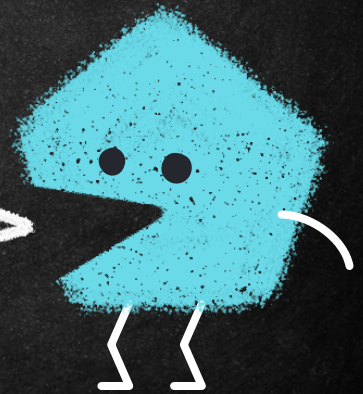
Possibilités

- ➜ Chiffrer le message à envoyer
- ➜ S’assurer de l’authenticité de l’expéditeur



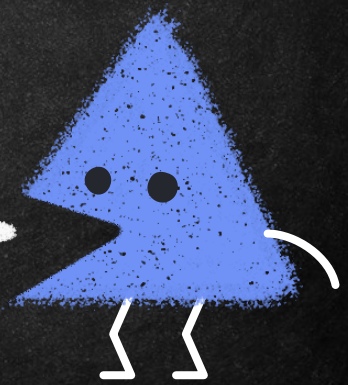
Les clés





Clé privée et clé publique

- Les deux clés sont liée mathématiquement
  - Nombres premiers
  - Elliptic Curve
- La clé publique est une fonction à un sens
- La clé privée est une brèche connu de cette fonction (Trap Door Function)
- Génération de la pair de clés



Récupération de la clé publique du destinataire

Clé publique de Garfield

Clé privée de Garfield

Chiffrement du message avec la clé publique du destinataire

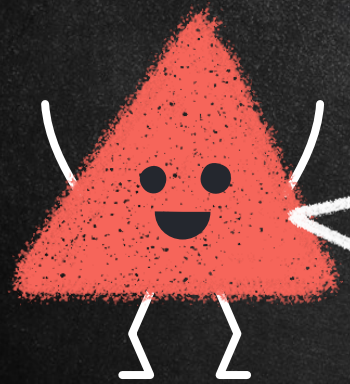
Lasagne aux kiwis

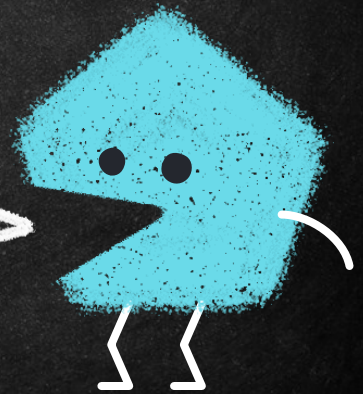
0xAk9uiVZ3

0xAk9uiVZ3

Lasagne aux kiwis

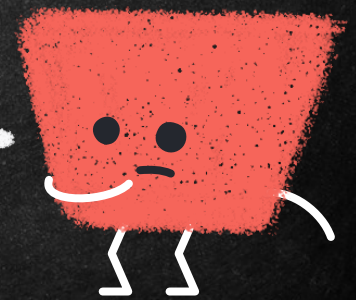
Formats des clés





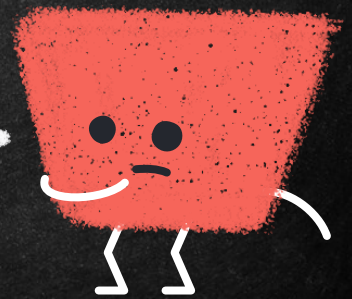
Formats des clés - PEM

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3gDIecx2M2FGHQ1zXj3W
0DxctyX+MINP7hkGJyI2lR4aZhnWNEocPqqb4C8v1cdlEXjC1cWTgxF1bcZxHAeP
CobTbvHZJdK/Sg83sbVh3sQbiPIbpggnH838qlMSYuHgnU/Hpntjem1TeH/4MIDb
cf4WS4rZ+id3vMzvXt0czMwvp0yBOFdANnKnOVWpwD114tPrjSoVSQ/uTyjHWnsd
hqqIFNULtYuIwgLc6ZHi6/7cER4L4vEcx4ADEuj0Bi1BOSgo3k235VDYAGG+Al4/
FDWEYIE3ne6rj/00NMjFrS5qQyJSIi8t1pp/3nQQXOlOmYKQvM+m2aW7amIZHaHi
qwIDAQAB
-----END PUBLIC KEY-----
```



Formats des clés - JWK

```
{
    "kty": "EC",
    "x": "jmqDxG1XjfzEJYPulwWCycdxqRGnz4xOtzytutTHUyc",
    "y": "GGpZUhS4q8rZCQpBODAjIDB9U4Yj4Xwbk9i1mUfOud8",
    "crv": "P-256"
}
```

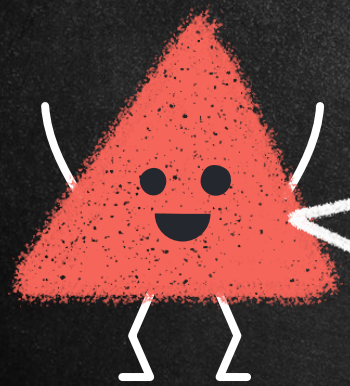


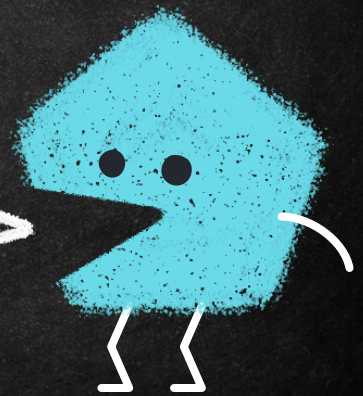
RSA

Ron Rivest

Adi Shamir

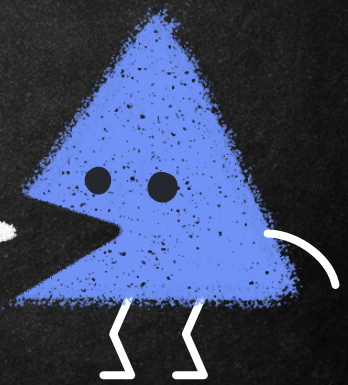
Leonard Adleman





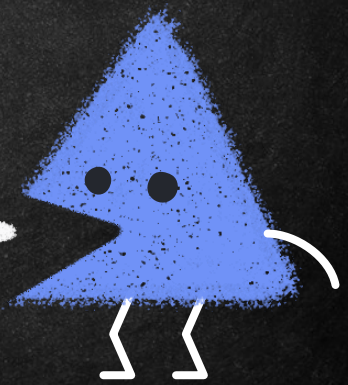
RSA

- L’algorithme le plus populaire
- Le principe est
  - La multiplication est rapide
  - La factorisation est lente
- Utilisation du modulo pour ne pas que les nombre deviennent trop gros



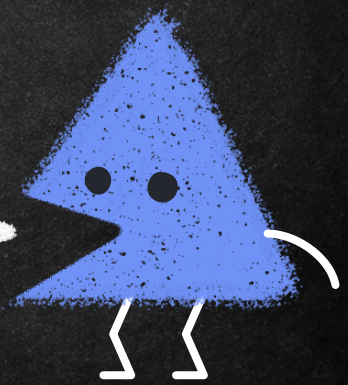
RSA

- Choix de deux nombres premiers aléatoires
- Max = le produit des deux nombres premiers
- Les clés privée et publique de nombres choisis tels qu'elles sont comprises entre 0 et max
- Voilà pourquoi la factorisation pourrait venir brisé RSA
  - Factoriser le max pour retrouver les deux nombres premiers permet de trouver la clé privée à partir de la clé publique



Exemple

- Nombres premiers: 13 et 7
- Max → 13 x 7 = 91
- Clé publique choix de 5 (0 < 5 < 91)
- Il faut trouver la brèche soit la clé privé pour ce faire : `Extended Euclidean algorithm`
  - Pour notre exemple : 29

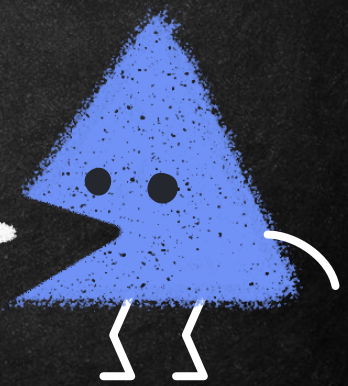


Exemple

- RSA(max: 91, pub: 5; priv: 29)
- Notre mot : CLOUD

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

- 67, 76, 79, 85, 68
- Dans Excel

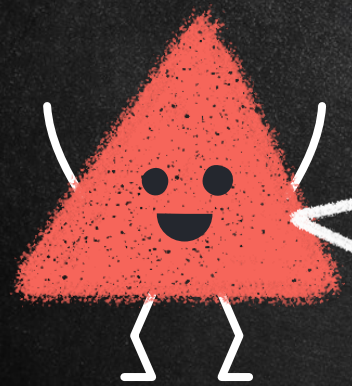


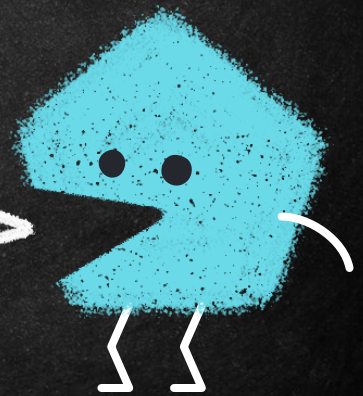
Inconvénients et limites

- ➜ Pas la *TrapDoor* parfaite
  - Factorisation est étudié depuis l'antiquité
  - Recherches en cours et informatique quantique
- ➜ Moins performants que leurs équivalents symétrique
  - Temps de chiffrement plus longs
  - Pour un niveau sécurité équivalent la clé doit être plus beaucoup plus longues
- ➜ La NSA serait en mesure de lire les messages

Elliptic curve

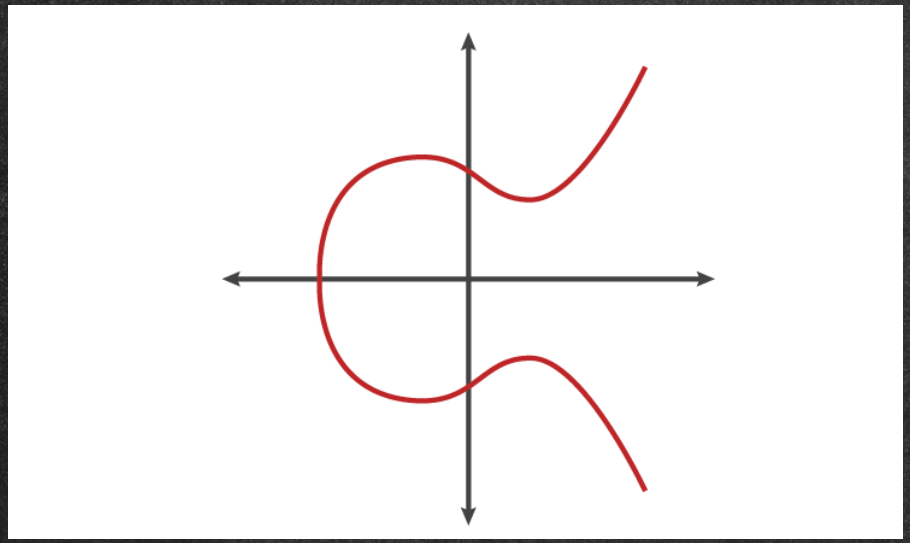
À la rescousse

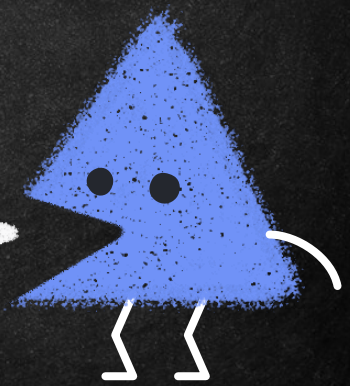




Elliptic Curve

$$y^2 = x^3 + ax + b$$





Différences

RSA

- La brèche devient de moins en moins difficile
- La taille de la clé devient de plus en plus longue
  - Briser 2048-bit clé, faire bouillir 1 cuillère d'eau

EC

- La brèche est un problème plus difficile
  - 30 ans de recherches aucun raccourci apparent
- Possible d'utiliser des clé plus courte
  - Briser 228-bit clé, faire bouillir toute l'eau de la Terre (2380 bits RSA)

Problème d'authenticité

À suivre