

La cryptographie

Introduction

La cryptographie existe depuis des milliers d'année. Voici quelque forme de cryptographie les plus ancienne au monde et/ou les plus utilisée :

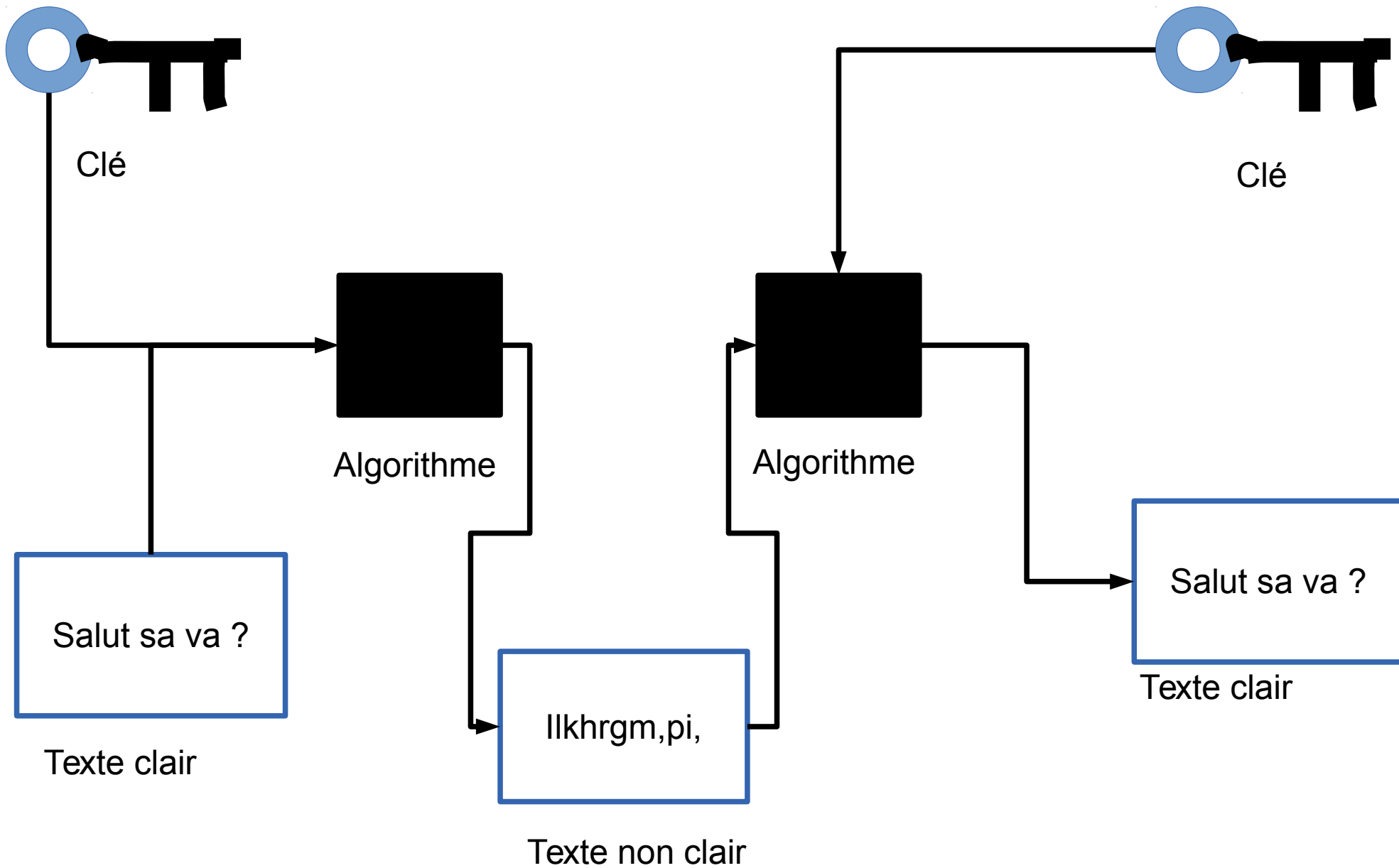
- l'egypte antique (2000 avant JC)
- Jules César (50 avant JC)
- code Enigma utilisé pendant la seconde guerre mondiale

Les clés

Clé non obligatoire mais rajoute une sécurité

Clé sécurisée implique une certaine longueur pour rendre les test exhaustifs trop longs pour être efficaces

Question de sécurité absolue, il faut tout de même donner la clé au récepteur avec un moyen qui doit être absolument sûr sinon toute la cryptographie est inutile



Exemple de message codé

On utilise plusieurs techniques de cryptographie :

Message de base : ceci est un message code

clé : abc

Message codé :
ciueceffothp*evougf*

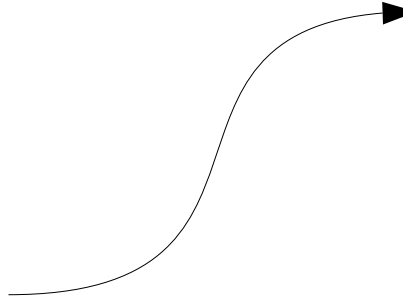
Processus :

Devient :

Décalage des
lettres :

ceciestunmessage
code

cfeifvuooetuahg
cpfe



Traitement par
colonnes :

cfe
ifv
uoo
etu
ahg
cpf
e**

Devient :



ciueceffothp*
evougf*

On remplace les
vides par des *

Conclusion

Problèmes des clés avec la puissance des machines évoluant à vitesse exponentielle
(2^{80} possibilité = minimum actuel)

Sources :

- http://www.esiee.fr/~bureaud/Unites/Saci1/tutoriel_g8/chiffrement1.html
- http://fr.wikipedia.org/wiki/Cryptographie_sym%C3%A9trique

Merci pour votre
attention