Série de TD n°3-2

Questions de compréhension :

1. Quelle est la différence entre un chiffrement de bloc et un chiffrement de flux ?
2. Combien de clés sont nécessaires pour que deux personnes puissent communiquer via un chiffrement ?
3. Quelles sont les deux fonctions de base utilisées dans les algorithmes de cryptage
4. Quelles sont les deux approches générales pour attaquer un chiffrement ?

Exercice 1

Expliquer à l'aide de schémas comment deux utilisateurs peuvent-ils échanger des informations chiffrées et authentifiées (chiffrement et signature). On utilisera par exemple les algorithmes AES, RSA et SHA

Exercice 2 (Chiffrement asymétrique : RSA)

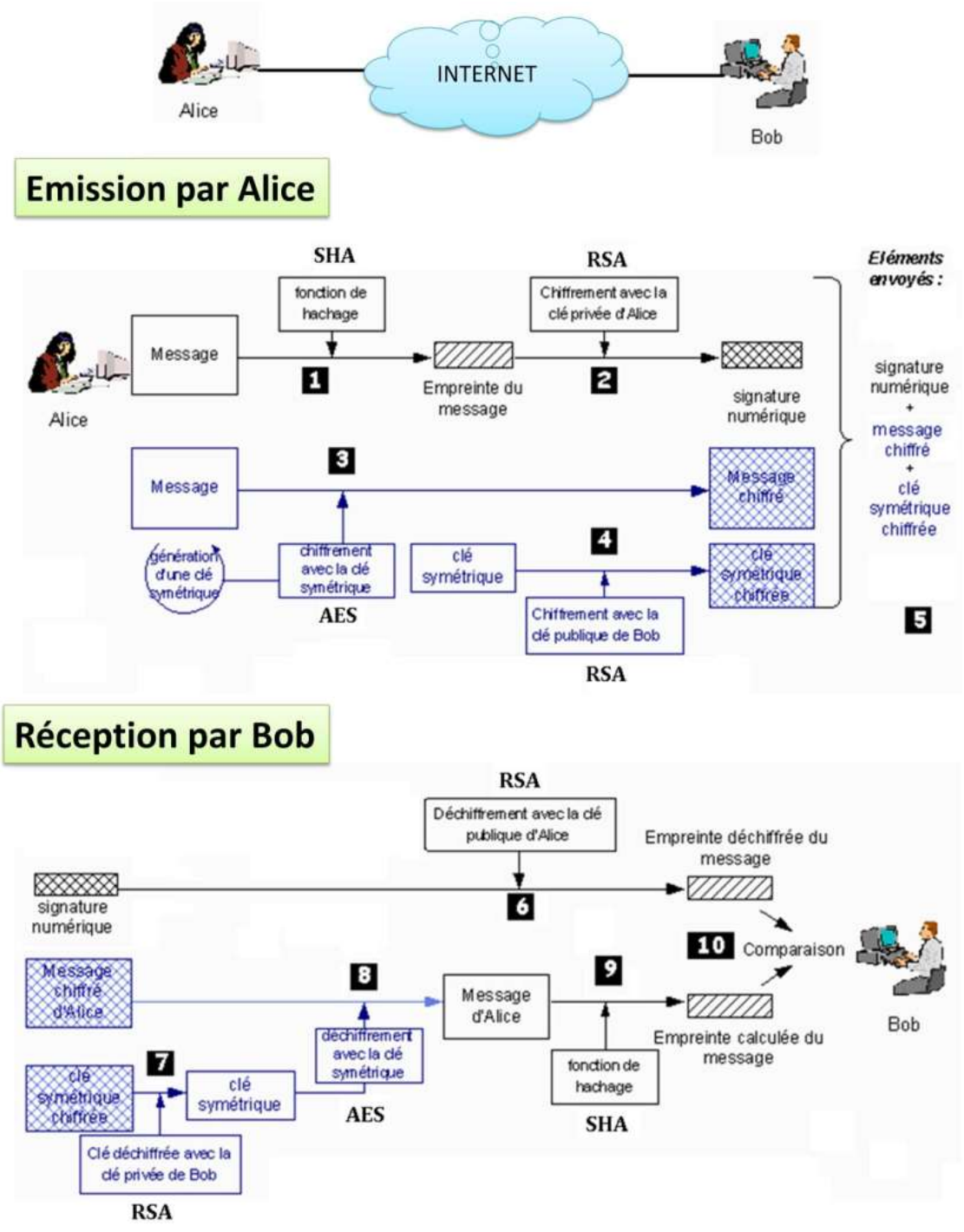
- Déchiffrer le message reçu M=18 chiffré avec la clé publique (35;11).
- Chiffrer le message M = 10 avec la clé publique (55;7). Calculer p; q et d. Déchiffrer C = 35.

Corrigé

<u>Questions de compréhension</u> :

1. Un chiffrement de flux est celui qui crypte un flux de données numériques un bit ou un octet à la fois. Un chiffrement de bloc est celui dans lequel un bloc de texte clair est traité comme un tout et utilisé pour produire un bloc de texte chiffré de même longueur.
2. Une clé pour les chiffres symétriques, deux clés pour les chiffres asymétriques.
3. Permutation et substitution.
4. Cryptanalyse et force brute.

Exercice 1



Exercice 2

Rappel des propriétés du calcul du modulo

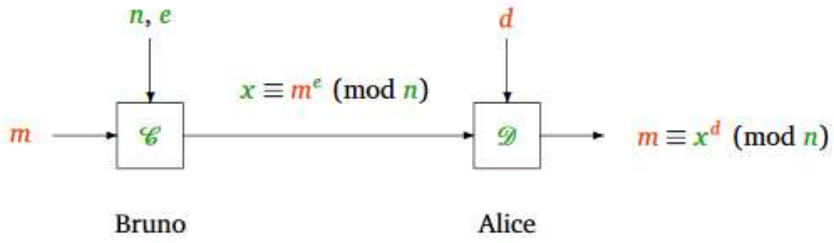
Lien 1 : https://commentcalculer.fr/calcul/modulo/

Lien 2 : https://www.maths-et-tiques.fr/telech/DivisibTS.pdf

Lien 3 : http://www.jaicompris.com/lycee/math/arithmetique/congruence-Z.php

Lien 4 : http://.free.fr/ThNbDemo/ModCongr.htm

Le schéma suivant récapitule le principe du chiffrement RSA :



Clés d'Alice :

- publique : n, e
- privée : d

- **Déchiffrer le message reçu 18 chiffré avec la clé publique (35;11).**

On a : $n = 35 = 5 \times 7 \Longrightarrow p = 5$ *et* $q = 7$

$\Phi(n) = (p-1)(q-1) = 4 \times 6 = 24$

e = 11 pour trouver d on a: $e \times d = 1 \ mod\ 24$, $d = e^{-1} \ mod\ 24 = 11^{-1} mod\ 24$

Donc $d = 11 \ mod\ 24$ (car $11 \times 11 = 1 \ mod\ 24$)

On déchiffre x =18 par le calcul suivant :

$m = x^d \ mod\ n = 18^{11} \ mod\ 35 = 2 \ mod\ 35$

Donc le message clair est m = **2**

- **Chiffrer le message m=10 avec la clé publique (55, 7)**

On a : e=7 et n= 55 donc $x = m^n = 10^7 mod\ 55 = 10 \ mod\ 55$

Donc le message chiffré est x = **10**

- **Calculer p; q et d.**

$n = 55 = 5 \times 11 \Longrightarrow \boldsymbol{p = 5}$ *et* $\boldsymbol{q = 11}$

$\Phi(n) = (p-1)(q-1) = 4 \times 10 = \mathbf{40}$

e = 7 pour trouver d on a: $e \times d = 1 \ mod\ 40$, $d = e^{-1} \ mod\ 40 = 7^{-1} mod\ 40$

Donc $\boldsymbol{d = -17 \ mod\ 40 = 23 \ mod\ 40}$

Donc p= **5**, q = **11** et d=**23**

- **Déchiffrer C = 35**

On déchiffre x =35 par le calcul suivant :

$m = x^d \ mod\ n = 35^{23} \ mod\ 55 = 30$

Le message clair est donc : m= **30**