Feuille de TD 1

Exercice 1. *1) Donner un exemple d'un code de substitution monoalphabétique et expliquer comment le cryptanalyser.*

2) Donner un exemple moderne *d'un code de permutation/transposition. Le processus est-il aisément réversible ?*

3) Qu'est qu'une fonction à sens unique *et comment sont-elles utilisées en cryptographie ?*

4) Qu'est qu'une fonction de hachage *? À quoi servent-elles et quelles doivent être leurs qualités ?*

5) Donner un exemple d'un registre à décalage *de longueur* 4 *et de périodicité maximale.*

Exercice 2. *Décoder le message suivant encodé par le protocole de Vigenère avec une clef de longueur* 2 *:*

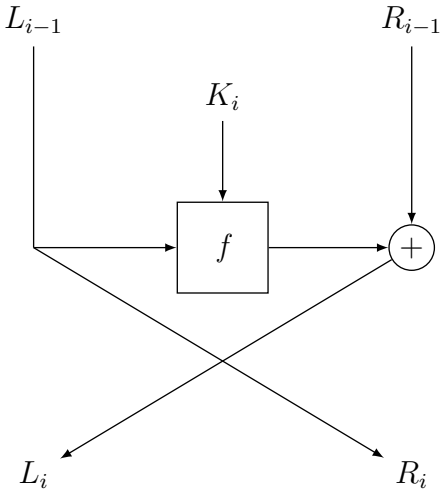
OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF

Exercice 3. *Bob utilise le protocole RSA et publie sa clé publique* $N = 187$ *et* $e = 3$.

1) Encoder le message $m = 15$ *avec la clé publique de Bob.*

2) En utilisant le fait que $\psi(N) = 160$*, retrouver la factorisation de* N *puis la clé privée de Bob.*

Exercice 4. *On rappelle qu'un schéma de Feistel est représenté sous la forme suivante.*



On considère alors un diagramme de Feistel à deux rondes sur des chaînes de 8 *bits avec deux fonctions* f_1 *et* f_2 *(associées à des clés* K_1 *et* K_2*) définies pour toute chaîne* a *de* 4 *bits par les formules suivantes :*

$$f_1(a) := a \oplus 1011 \qquad et \qquad f_2(a) := \overline{a} \oplus 0101,$$

où $\overline{a}$ *désigne la négation de* a*, i.e.* $a + \overline{a} = 1111$*.*

1) *Calculer l'image de la chaîne* 11010011 *par ce diagramme.*
2) *Déterminer une chaîne de* 8 *bits dont l'image par le diagramme est elle-même.*
3) *La propriété précédente, l'existence d'une chaîne invariante par le diagramme de Feistel, est-elle vraie pour toutes les fonctions* f_1 *et* f_2 *?*

Exercice 5. *On considère un chiffrement du type El Gamal pour* $p = 23$*. On admettra que* 5 *est un générateur de* $\mathbb{F}_{23}^{\times}$*. Alice choisit* 10 *comme clef secrète.*

1) *Quelle est la clef publique d'Alice ?*
2) *Alice reçoit le message* $(20, 22)$ *codé avec sa clef publique, où le second membre,* 22*, est le masquage du message en clair. Après avoir rappelé le principe du codage, décrypter ce message.*