Université de Perpignan Année 2012-2013
M. François, C. Negre

Examen de Cryptographie
Master EAI 1

Recommandation: *Notes de cours et de TD autorisées. Calculatrice autorisée. La qualité de la rédaction sera prise en compte dans la correction de la copie.*

Exercice 1. 1. *Chiffrement de Vigenère.*

(a) Numérisez avec la correspondance $a \leftrightarrow 0, b \leftrightarrow 1, \ldots, z \leftrightarrow 25$ le message suivant

Ceci est un secret

(b) Chiffrez le avec un chiffrement de Vigenère et la clef $k = (4, 17, 23)$.

2. *Chiffrement par substitution.*

(a) On considère les substitutions qu'on peut qualifiée de bi-cycle: on découpe l'alphabet numérisé $[0, 25]$ en deux intervalles $I_1 = [0, \lambda_1 - 1]$ et $I_2 = [\lambda_1, 25]$. Sur l'intervalle I_1 on effectue un décalage cyclique de k_1 et sur I_2 de k_2. Cette substitution peut s'écrire:

$$S(\lambda) = \begin{cases} (\lambda + k_1) \mod \lambda_1 & \text{si} \quad \lambda \in I_1 \\ ((\lambda - \lambda_1 + k_2) \mod (26 - \lambda_1)) + \lambda_1 & \text{si} \quad \lambda \in I_2 \end{cases}$$

Chiffrez le message de la question 1.a pour la substitution donnée par $\lambda_1 = 7$ et $k_1 = 3$ et $k_2 = 11$.

(b) On considère le message suivant chiffré avec une substitution bi-cycle

begytwovkyewlmiizobiophihizoigldmxpizxpmwiyciooidohiwyvoikiybmd
jvyceomvdiobizgvccpdgeomvdzidoiycizhigvdjmhidomebmoihepolidomgm
oiiohmdoikymoipdiwiyzvddiwyeomxpedobegytwovkyewlmiizoewwibiipdg
ytwovkyewlipdimdjvyceomvdhvdobegvdjmhidomebmoidizowezwyvoikiiiz
oewwibiioisoigbemyoedhmzxpibmdjvyceomvdwyvoikiiizoewwibiioisoig
lmjjyibewbpweyohizebkvymolcizgytwokyewlmxpizhiwidhidohpdweyecio
yizigyioewwibibegbij

les fréquences des lettres sont les suivantes:

a	b	c	d	e	f	g	h	i	j	k	l	m
0.000	0.047	0.022	0.072	0.072	0.000	0.035	0.035	0.180	0.020	0.022	0.020	0.067
n	o	p	q	r	s	t	u	v	w	x	y	z
0.000	0.115	0.032	0.000	0.000	0.005	0.010	0.000	0.047	0.067	0.012	0.067	0.042

déterminer la substitution bi-cycle qui a servie à chiffrer le message et déchiffrer le début du message. (Indication s'aider du "e" et de la séquence des lettres de l'alphabet v,w,x,y,z qui ont des fréquences quasi nulles).

Exercice 2 (Chiffrement symétrique moderne)**.** On considère le SPN décrit dans l'annexe. La boite S est donnée par

X	$[0,0,0,0]$	$[0,0,0,1]$	$[0,0,1,0]$	$[0,0,1,1]$	$[0,1,0,0]$	$[0,1,0,1]$	$[0,1,1,0]$	$[0,1,1,1]$
$S(X)$	$[0,1,1,0]$	$[1,0,0,1]$	$[1,1,0,0]$	$[0,0,1,1]$	$[0,0,0,1]$	$[1,1,1,0]$	$[1,0,1,1]$	$[0,1,0,0]$
X	$[1,0,0,0]$	$[1,0,0,1]$	$[1,0,1,0]$	$[1,0,1,1]$	$[1,1,0,0]$	$[1,1,0,1]$	$[1,1,1,0]$	$[1,1,1,1]$
$S(X)$	$[1,1,0,1]$	$[0,0,1,0]$	$[0,1,1,1]$	$[1,0,0,0]$	$[0,0,0,0]$	$[1,0,1,0]$	$[1,1,1,1]$	$[0,1,0,1]$

et toutes les clefs de ronde sont toutes égales à la clef de chiffrement $K \in \{0,1\}^{12}$.

1. Déchiffrez le bloc $C = [111001110110]$ en utilisant la clef $K = [101011110111]$.

2. Chiffrer le bloc $M = [011111110110]$ en utilisant la clef $K = [101011110111]$ avec le mode CBC.

3. On considère les deux propagations de différence suivantes pour la boîte S

$$\begin{array}{llllll} \Delta_0 \to \Delta_0^\star \text{ avec} & \Delta_0 & = & [0,0,1,1], & \Delta_0^\star & = & [0,1,0,1], \\ \Delta_1 \to \Delta_1^\star \text{ avec} & \Delta_1 & = & [0,0,1,0], & \Delta_1^\star & = & [1,0,1,0]. \end{array}$$

   Sur le diagramme décrit dans l'annexe, en partant de la boite S à gauche de la première ronde et du deuxième couple $\Delta_0 \to \Delta_0^\star$ et $\Delta_1 \to \Delta_1^\star$ de la question précédente, déterminez une propagation de différence entre un couple de message clair et le couple partiellement chiffré sortant de la 3ème ronde.

4. Sachant que les probabilité $\Delta_0 \to \Delta_0^\star$ et $\Delta_1 \to \Delta_1^\star$ des propagations pour S valent

$$p_{\Delta_0 \to \Delta_0^\star} = 1 \text{ et } p_{\Delta_1 \to \Delta_1^\star} = 3/4.$$

   calculer la probabilité de la propagation de différence sur les trois première ronde décrite dans la question précédente.

5. Décrire une attaque différentielle basée sur la propagation de différence trouvée: vous décrirez le processus général, les bits de la clef que cela permet de calculer, le nombre et le type de couples de message clair-chiffré nécessaires.

Exercice 3 (Cryptographie à clef publique)**.** On considère la clef publique RSA $N = 319$ et $e = 11$.

1. Appliquer l'algorithme d'exponentiation rapide en détaillant les calculs pour chiffrer le message $m = 119$.

2. Donner un majorant pour le plus petit facteur de N, puis factoriser N.

3. Déterminer l'exposant de déchiffrement d en détaillants vos calculs.

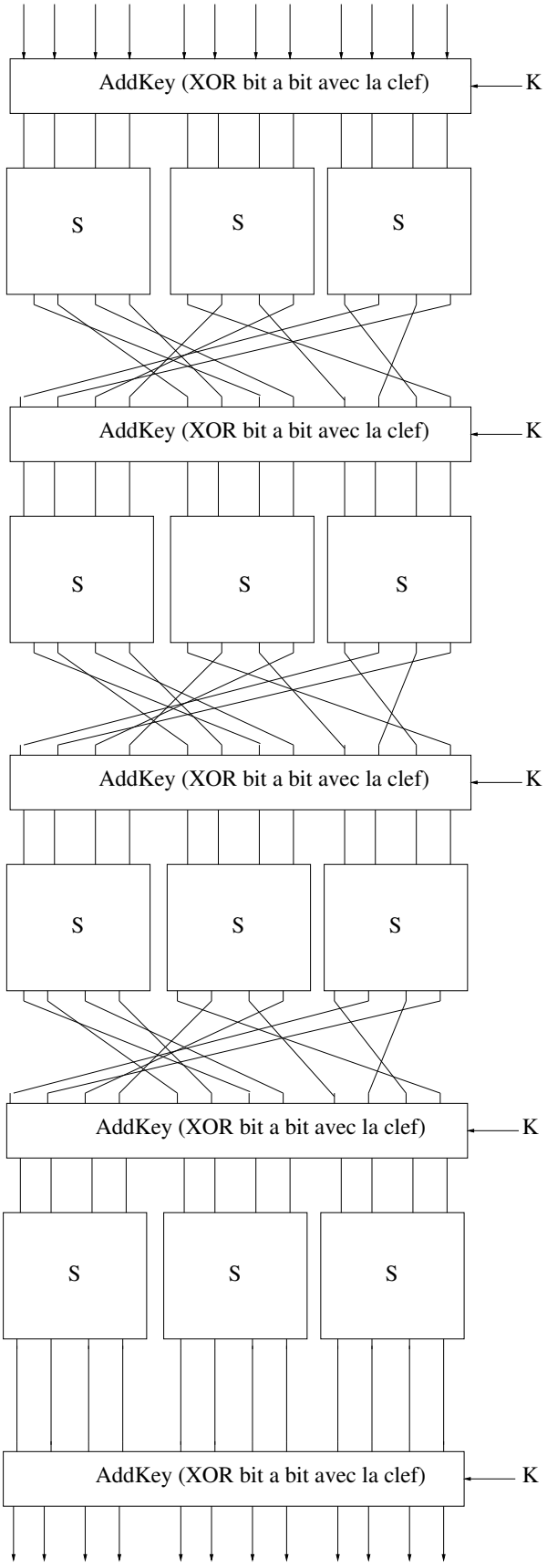
Exercice 4 (Attaque pas de bébé, pas de géant)**.**

1. Rappeler le principe de l'attaque.

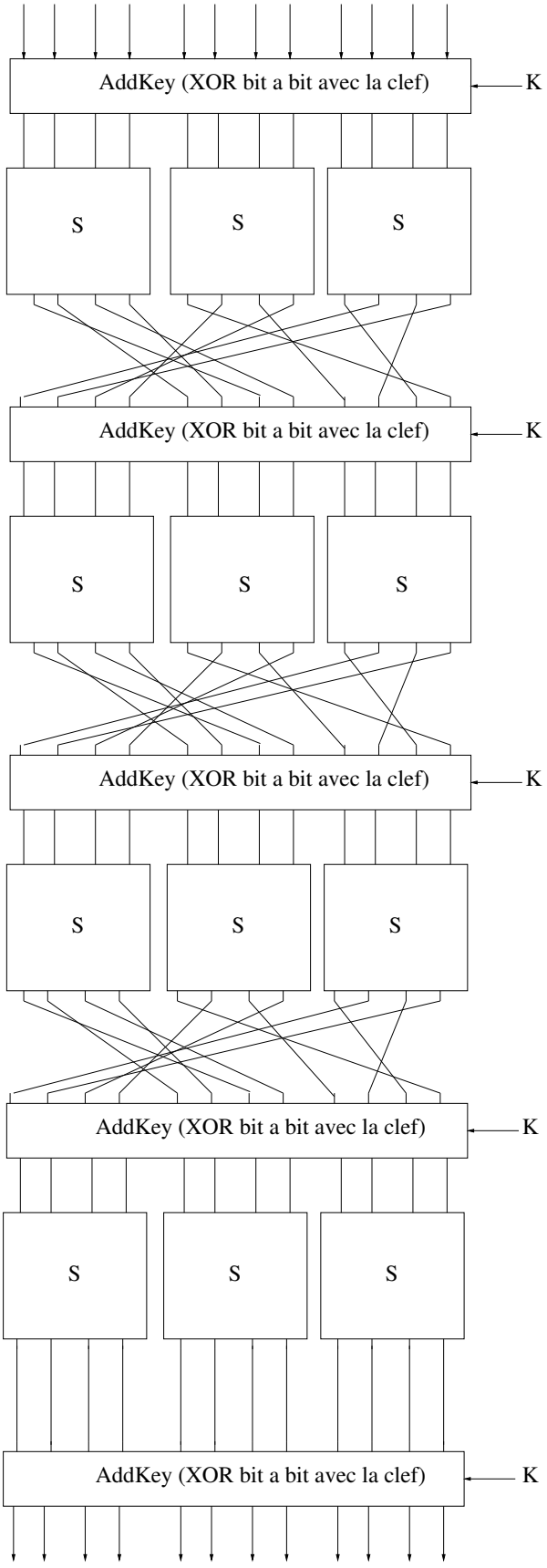
2. On considère l'entier premier $p = 907$ et un générateur $g = 2$, en utilisant les éléments ci-dessous calculer le log discret de $A = 787$ en base g.

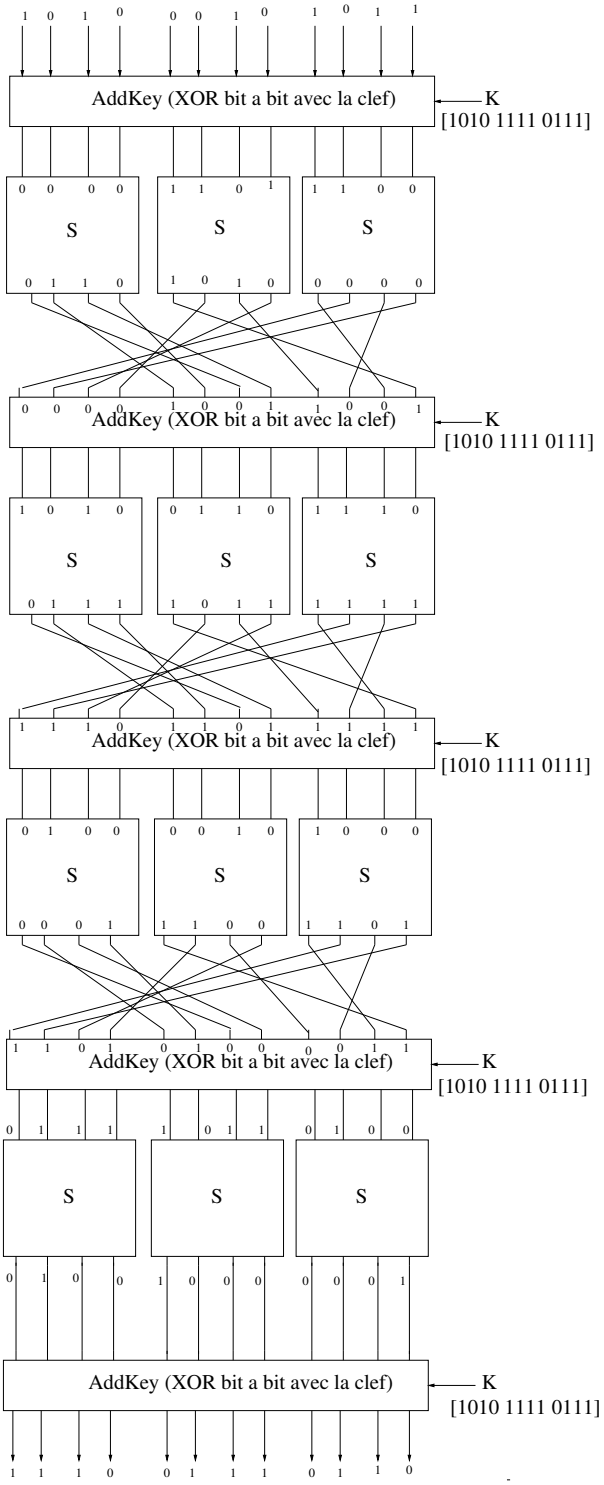
$$\begin{array}{llllllll} g^{31*0} \mod p = 1, & g^{31*1} \mod p = 609, & g^{31*2} \mod p = 825, & g^{31*3} \mod p = 854, \\ g^{31*4} \mod p = 375, & g^{31*5} \mod p = 718, & g^{31*6} \mod p = 88, & g^{31*7} \mod p = 79, \\ g^{31*8} \mod p = 40, & g^{31*9} \mod p = 778, & g^{31*10} \mod p = 348, & g^{31*11} \mod p = 601, \\ g^{31*12} \mod p = 488, & g^{31*13} \mod p = 603, & g^{31*14} \mod p = 799, & g^{31*15} \mod p = 439, \\ g^{31*16} \mod p = 693, & g^{31*17} \mod p = 282, & g^{31*18} \mod p = 315, & g^{31*19} \mod p = 458, \\ g^{31*20} \mod p = 473, & g^{31*21} \mod p = 538, & g^{31*22} \mod p = 215, & g^{31*23} \mod p = 327, \\ g^{31*24} \mod p = 510, & g^{31*25} \mod p = 396, & g^{31*26} \mod p = 809, & g^{31*27} \mod p = 180, \\ g^{31*28} \mod p = 780, & g^{31*29} \mod p = 659, & g^{31*30} \mod p = 437, & g^{31*31} \mod p = 382. \end{array}$$

Annexe de l'exercice 2 - question 1.



Annexe de l'exercice 2 - question 3.




AddKey (XOR bit a bit avec la clef)
K
[1010 1111 0111]
S
S
S
AddKey (XOR bit a bit avec la clef)
K
[1010 1111 0111]
S
S
S
AddKey (XOR bit a bit avec la clef)
K
[1010 1111 0111]
S
S
S
AddKey (XOR bit a bit avec la clef)
K
[1010 1111 0111]
S
S
S
AddKey (XOR bit a bit avec la clef)
K
[1010 1111 0111]