Cryptographie avancée - TP1

Anne Garcia-Sanchez

M2i - CFA CCI Avignon - 10 septembre 2024

Encodage - Chiffrements symétriques

1 Encodage

Les messages que nous allons lire peuvent être encodés de différentes façons.

1. Décoder le message `b'd\xc3\xa9cod\xc3\xa9!'`

2. - Écrire une fonction qui traduit un message en ascii (ou UTF-8)
   Exemple: 'hello' devient 104 101 108 108 111

   - Écrire une fonction qui décode un message encodé UTF-8 et décoder le message suivant:
   66 114 97 118 111 44 32 116 111 117 116 32 118 97 32 98 105 101 110 33

3. - Écrire une fonction qui encode un message en binaire: chaque caractère est codé sur 8 bits.
   Exemple: 'hello' devient 01101000011001010110110001101100011011111

   - Écrire une fonction qui décode un message binaire et décoder le message suivant:
   01000101011101000010000001110110011011110110100101101100011000010010000 1

4. - Écrire une fonction qui encode un message en hexadécimal.
   Exemple: 'hello world' devient 68656C6C6F20776F726C64

   - Écrire une fonction qui décode et décoder le message: 53616C7574206C6573206861636B65727321

5. - Utiliser la librairie python `base64` pour écrire une fonction qui encode un message en base64.
   Exemple: 'Hello world!' devient SGVsbG8gd29ybGQh

   - Écrire une fonction qui décode et décoder le message: RmluIGRlIGwnZXhvMTogYnJhdm8h

2 Chiffrement par substitution: Chiffre ROT47

Écrire une fonction `encryptROT47(plaintext)` qui chiffre ou déchiffre en ROT47.

Déchiffrer le message: '`y6 DF:D #~%cfi ;6 E@FC?6 DFC hc 42C24E6C6DP`'

3 DES-AES

1. Utiliser la librairie `PyCryptodome` pour déchiffrer le message suivant chiffré en simple DES avec le mode CBC, la clé `b'8bytes k'` et le vecteur d'initialisation `b'\xcb\xb3\xc9p~\x027\xc9'`

   `b'\xf7;\\\xff\xd7yg\xe6\x02P\x0f\xdd\x1b\xeb\xec\xe5'`

2. Déchiffrer le message suivant chiffré avec l'AES en mode GCM avec la clé `b'super grande cle'` et le nonce `b'cn\xcd\x1d\xab\xff?\xd3OK\x96z'`

   `b')\x08\x87\xc3/\x18\x11\x83%\xa3‘\xf8\xd6\xa6\x88\xa2@f$\xce\xad\x89\xf4'`

4 Bonus - Chiffrements par transposition (ou permutation)

Une transposition peut être définie par une permutation sur un bloc de taille donnée.

Exemple: permutation [3, 6, 5, 1, 4, 2]

clair	1	2	3	4	5	6
	S	E	C	R	E	T
chiffré	3	6	5	1	4	2
	C	T	E	S	R	E

Écrire une fonction qui chiffre un message en appliquant la transposition passée en argument.
Le message correspondra à un bloc: il sera exactement de la taille de la transposition.

Déchiffrer le message `'r oneggéeacn'` avec la permutation [5, 7, 4, 2, 6, 10, 8, 12, 1, 9, 3, 11]

bonus 1: prévoir le cas où le message correspond à plusieurs blocs entiers.
Déchiffrer le message `'rueo encctneer soé vlidé'` avec la permutation [5, 8, 1, 4, 7, 6, 2, 3]

bonus 2: prévoir le cas où le dernier bloc n'est pas complet et le compléter avec des lettres prises dans l'ordre alphabétique.

Déchiffrer le message: `ivetlEsloameapeugsrscvlaleeseesrstdtlneaeddraoecrb`
avec la permutation [5, 3, 9, 2, 6, 1, 10, 8, 4, 7]