

TD Cryptographie:

Exercice 1 :

A->J	B->X	C->Z	D->W	E->V	F->B	G->R	H->T	I->H	J->N	K->D	L->P	M->Y
N->Q	O->U	P->M	Q->G	R->O	S->I	T->S	U->L	V->F	W->C	X->E	Y->A	Z->K

- 1) Avec la table de substitution précédente, chiffrez le texte suivant :
 - BLABLATESTINGBLABLABLAOVER
- 2) Sachant que les textes suivants ont été chiffrés avec la matrice de substitution précédente, déchiffrez les:
 - HPAJMJIWVSWZOAMSU
 - STVJOSUBZUYMLSVOMOMOUROJYYHQR

Exercice 2 AES :

- 1) Donnez la représentation polynomiale des chiffres suivants dans $FF(2^8)$:
 - 56
 - 237
 - 234
 - 215
- 2) Calculez la multiplication dans $FF(2^8)$ des deux polynômes suivants (polynôme premier de réduction = $x^8+x^4+x^3+x+1$) :
 - 234×215
 - $P = 234 \times 37$
 - $215 \times P$
- 3) Calculez la multiplication dans $FF(2^8)$ des deux polynômes suivants (polynôme premier de réduction = $x^8+x^4+x^3+x+1$) :
 - 157×220
 - $P = 157 \times 90$
 - $220 \times P$

Exercice 3 RSA :

- Chiffrez la valeur $x = 87$ avec RSA ; clé publique = (N=253, E=17)
- Déchiffrez la valeur $x = 54$ avec RSA ; clé privé = (N=253, E=13)