

Nom: Boukhenifra
Prénom: Nadhir
Spécialité: Cryptographie et Sécurité (CS) – Master 2
module: Cryptographie Avancée

Université: Batna 2 - Chahid Mostefa BEN BOULAID.
Faculté: Mathématiques et d'Informatique
Département: Informatique
Année universitaire: 2018/2019

Rapport : One-Time Pad Cryptage et Décryptage

Le chiffrement "one-time pad" Ce système est aussi appelé chiffrement à flot ou clé-une-fois ou masque jetable ou chiffre de Vernam, du nom de son inventeur G. Vernam. Celui-ci a mis en forme en 1917 une idée remontant en fait à 1882 (F. Miller).

En 1919, Vernam a breveté un système électromécanique réalisant ce cryptage. Essentiellement, le chiffrement de Vernam répond au même principe que le Vignère. Il effectue une addition modulaire du message clair M avec une clé K pour obtenir le chiffré C : $C = M \oplus K$.

- M: Suit Binaire 1001011... (Plein Texte (Message En Clair))
- K: Suite Binaire De Même Longueur Que M (Clé)
- Chiffrement De $M' = M \oplus K$ (XOR)
- Test: Le Cryptage et Le Décryptage
- Application: Chiffrée Un Logo (En Noire Et Blanc)

Test:

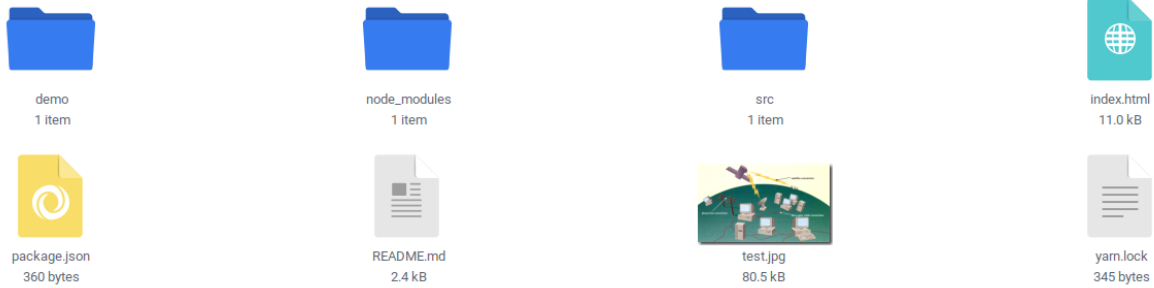
Cryptage $M' = M \oplus K$ (XOR)	Décryptage $M = M' \oplus K$ (XOR)
M = 01101 K = 10101 $0 \wedge 1 = 1$ $1 \wedge 0 = 1$ $1 \wedge 1 = 0$ $0 \wedge 0 = 0$ $1 \wedge 1 = 0$ M' = 11000	M' = 11000 K = 10101 $1 \wedge 1 = 0$ $0 \wedge 1 = 1$ $1 \wedge 0 = 1$ $0 \wedge 0 = 0$ $1 \wedge 0 = 1$ M = 01101

Application:

\$ cd /ACPWOTP/ && google-chrome index.html

Ce travail est publié dans une plateforme GitHub:
<https://github.com/NadhirBoukhenifra/ACPWOTP>

1. Structure de dossier



2. Cryptage et Décryptage Text

[illegible]

One-Time PAD - Decrypt Text

KT = Key Text

痧狻虛樵吳割b痲崙奎傾□梨□撈耳□廖談黠滄莖*巷御t蜚肅掄：罍湛醒□茲q

TC = Encrypted Text

痲焚藝樺嗎q叩痺崗林判□署□扶襄□掖貽詭梨豎q戛文k暫腹撲：〰潜齒□玆q

Decrypt

T = KT ^ TC = Decrypted Text

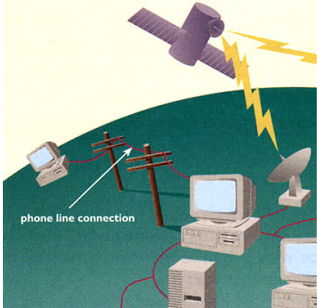
Hello, World!
مرحبًا يا عالم.
2019 <3

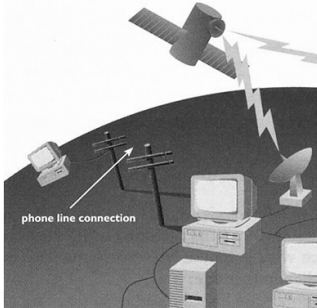
3. Cryptage et Décryptage Image

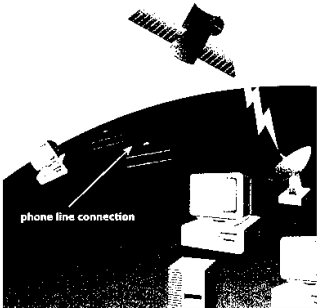
One-Time PAD - [Encrypt](#) Image (Black&White)

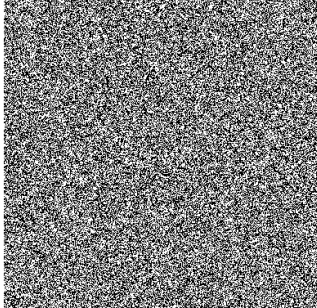
Image to Encrypt!

Upload Image









K = Binary Key

1111010010111010101101110000011101011110111100111000110100000001011011100000101100110001010110100011010000100110010011000000010011000001110101100011011110001011101101001101010001000001101010000010000100001101100001001101011110010011000100001100010010101101001001010111100010000111001100110001100110101011100010000111001100110001100110101

One-Time PAD - [Decrypt](#) Image (Black&White)

Image to Decrypt!

Upload Image

K = Binary Key

111101001011101010110111000001110101111011110011100011010000000101101110000010110011000101011010001101000010011001001100000001001100000111010110001101111000101110110100110101000100000110101000001000010000110110000100110101111001001100010000110001001010110100100101011100010000111001100110001100110101

