POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420a: Sécurité Informatique
Exercice séance 2 : Cryptographie 1

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Exercice 1 : Calcul d'entropie

- Objectif
  - Savoir évaluer l'entropie d'une source

Exercices de crypto

- Exercice 1 : Calcul d'entropie

- Vous avez une source sans mémoire qui sort un résultat pile ou face
- La source sort pile avec une proportion de 90 % et face avec une proportion de 10 %
- Vous placez 10 entrées dans un tampon (buffer) et vous voulez calculer l'entropie dans ce tampon

Exercices de crypto

- Exercice 1 : Calcul d'entropie

- Question 1 : quelle est l'entropie de ce tampon ?
  1. 1.11 bits
  2. 3.32 bits
  3. 4.69 bits
  4. 10 bits

Exercices de crypto

- Exercice 1 : Calcul d'entropie
- Réponse question 3 :
  3. 4,69 bits
- Définition de l''entropie de Shannon d'une source :
  - $H(S) = \sum_i p_i \log_2 (1/p_i)$ avec $1 \leq i \leq N$
- Entropie de notre source :
  - $H(S) = 0,1 * \log_2 (1/0,1) + 0,9 * \log_2 (1/0,9)$
  - $H(S) = 0,1 * 3,32 + 0,9 * 0,152 = 0,332 + 0,137 = 0,469$ bit
- Entropie de notre tampon
  - S^b : source obtenue en mettant b symboles de S dans un tampon
  - Si S est markovien, alors $H(S^b) = b*H(S) = 10 * 0,469 = 4,69$ bits

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Exercice 2 : Entropie d'un mot de passe

- Objectif
  - Savoir calculer l'entropie d'un mot de passe
  - Savoir calculer la probabilité de casser un mot de passe

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Exercice 2 : Entropie d'un mot de passe

- Vous avez conçu un site proposant une application pour téléphone qui exige un nombre de 6 caractères alphanumériques pour un mot de passe (minuscules, majuscules et chiffres)
- On suppose que les usagers choisissent leur mot de passe de manière aléatoire, avec tous les caractères étant équiprobables
- Cependant, comme les utilisateurs doivent entrer leur mot de passe au téléphone, le quart des usagers utilisent un mot de passe composé uniquement de chiffres

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Exercice 2 : Entropie d'un mot de passe

- Question 1 : Calculez l'entropie moyenne du mot de passe choisi par les usagers
  1. Environ 20 bits
  2. Environ 26 bits
  3. Environ 32 bits
  4. Environ 36 bits

Exercices de crypto

- Réponse question 1 :
- Pour les usagers ayant choisi uniquement des chiffres
  - Entropie de la source correspondant à chaque chiffre :
    - $H(S) = \sum_i p_i \log_2 (1/p_i)$ avec $0 \leq i \leq 9$
    - $H(S) = 10 * 0{,}1 \log_2 (1/0{,}1) = \log_2 (10)$ (chaque chiffre est équiprobable)
    - H(S) = 3,322 bits
  - Entropie de la source correspondant au mot de passe
    - H(S) = 6 * 3,322 = 19,93 bits (source markovienne)
  - Remarque : on peut calculer ça différemment
    - Il y a 1000000 mots de passe possibles soit 10^6 combinaisons possibles
    - 10^6 ≈ 2^20
    - Un mot de passe correspond à une clé sur approximativement 20 bits
    - Donc l'entropie correspond à approximativement 20 bits

Exercices de crypto

- Réponse question 1 :
- Pour les usagers ayant choisi un mot de passe alphanumérique
  - Entropie de la source correspondant à chaque caractère :
    - $H(S) = \sum_i p_i \log_2 (1/p_i)$ avec $1 \leq i \leq 62$ (26 + 26 +10)
    - $H(S) = \log_2 (62) = 5{,}954$
  - Entropie de la source correspondant au mot de passe
    - H(S) = 6 * 5,954 = 35,72 bits (source markovienne)
  - On vérifie le calcul différemment
    - Il y a maintenant 62^6 combinaisons possibles
    - 62^6 = 56 800 235 584 ≈ 56,8 * 10^9 ≈ 56,8 * 2^30 ≈ 2^6 * 2^30 = 2^36
    - Un mot de passe correspond à une clé sur approximativement 36 bits
    - Donc l'entropie correspond à approximativement 36 bits

Exercices de crypto

- Réponse question 1 :

- Entropie de la source qui génère les mots de passe
  - Correspond à une source markovienne qui génère aléatoirement ¼ de mot de passe numérique et ¾ de mots de passe alphanumérique
  - H(S) = ¼ * 19,93 + ¾ * 35,72 = 31,77 bits

  - Attention : c'est différent d'une source qui générerait un chiffre dans ¼ des cas et un caractère alphanumérique dans ¾ des cas

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Vous êtes informés que plusieurs dizaines d'usagers se sont fait pirater leur application
- Un ordinateur est pris en flagrant délit d'usage d'un compte piraté
- L'investigation forensic de l'ordinateur permet de découvrir un maliciel qui transformait l'ordinateur en membre d'un réseau de zombis (botnet)
- L'investigation découvre aussi un script pour réaliser une attaque de force brute sur l'authentification de votre site

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de crypto

- Le réseau de botnet peut contenir 25 000 ordinateurs infectés
- Chacun ordinateur peut tenter 10 mots de passe par minute
- On suppose que l'attaquant dispose de la liste des noms d'usager
- Mais il ne sait pas quel usager a choisi un mot de passe numérique ou alphanumérique

Exercices de crypto

- Question 2 : calculez le nombre de mots de passe composés d'une suite de 6 chiffres qui seront en moyenne cassés par jour (au minimum)
  1. Environ 50
  2. Environ 90
  3. Environ 120
  4. Environ 180

Exercices de crypto

- Réponse question 2 :
  - Nombre de mots de passe testés par un ordinateur par jour
    - 10 * 60 * 24 = 14400 mots de passe par jour
  - Nombre de mots de passe testés par le botnet par jour
    - 14400 * 25000 = 360 000 000 = 36 * 10^7 mots de passe par jour
  - Supposons que ces 36 * 10^7 mots de passe sont envoyés aléatoirement à l'ensemble des usagers du site
  - Il y aura ¼ de ces mots de passe qui seront envoyés à des usagers ayant choisi un mot de passe numérique, soit 9 * 10^7 mots de passe
  - Pour casser un mot de passe numérique, il faut 10^6 tentatives (cas pire)
  - L'attaquant va donc pouvoir casser le mot de passe de 90 usagers

Exercices de crypto

- Réponse question 2 :
  - Remarque : s'il y a beaucoup d'usagers, il vaut mieux tester aléatoirement quelques mots de passe sur chaque usager
  - Statistiquement, la loi des grands nombres s'appliquent et l'attaquant parviendra à casser des mots de passe même s'il n'envoie que quelques tentatives sur chaque compte
  - Par contre, l'attaque sera beaucoup plus furtive

Exercices de crypto

- Exercice 3 : Analyse fréquentielle de cryptogramme

- Objectifs :
  - Comprendre les limites du chiffrement mono-alphabétique
  - Savoir réaliser une analyse fréquentielle

Exercices de crypto

- Exercice 3 : Analyse fréquentielle de cryptogramme

- Cassez un cryptogramme qui utilise une substitution mono-alphabétique
- Le texte en clair est en français et ne contient que des lettres
- C'est un extrait d'une fable de La Fontaine

Exercices de crypto

- Question 1 : Cassez le cryptogramme suivant,

gcxobwryv ib ogx tb syiib
ypsyxg ib ogx tbv qmgzev
t cpb wgqrp wrox qysyib
g tbv obiybwv t roxrigpv
vco cp xgeyv tb xcojcyb
ib qrcsbox vb xorcsg zyv
ab igyvvb g ebpvbo ig syb
jcb wyobpx qbv tbcd gzyv
ib obfgi wcx wrox mrppbxb
oybp pb zgpjjcgyx gc wbvxyp

Exercices de crypto

- Indication question 1

- Vous pouvez trouver des sites qui calculeront la fréquence d'apparition des caractères dans un texte
- Voir par exemple :
  - https://www.dcode.fr/analyse-frequences

- Pour plus d'information sur l'analyse fréquentielle du français, voir par exemple :
  - https://fr.wikipedia.org/wiki/Analyse_fr%C3%A9quentielle

Exercices de crypto

- Réponse question 1 :

AUTREFOIS LE RAT DE VILLE
INVITA LE RAT DES CHAMPS
D UNE FACON FORT CIVILE
A DES RELIEFS D ORTOLANS
SUR UN TAPIS DE TURQUIE
LE COUVERT SE TROUVA MIS
JE LAISSE A PENSER LA VIE
QUE FIRENT CES DEUX AMIS
LE REGAL FUT FORT HONNETE
RIEN NE MANQQUAIT AU FESTIN

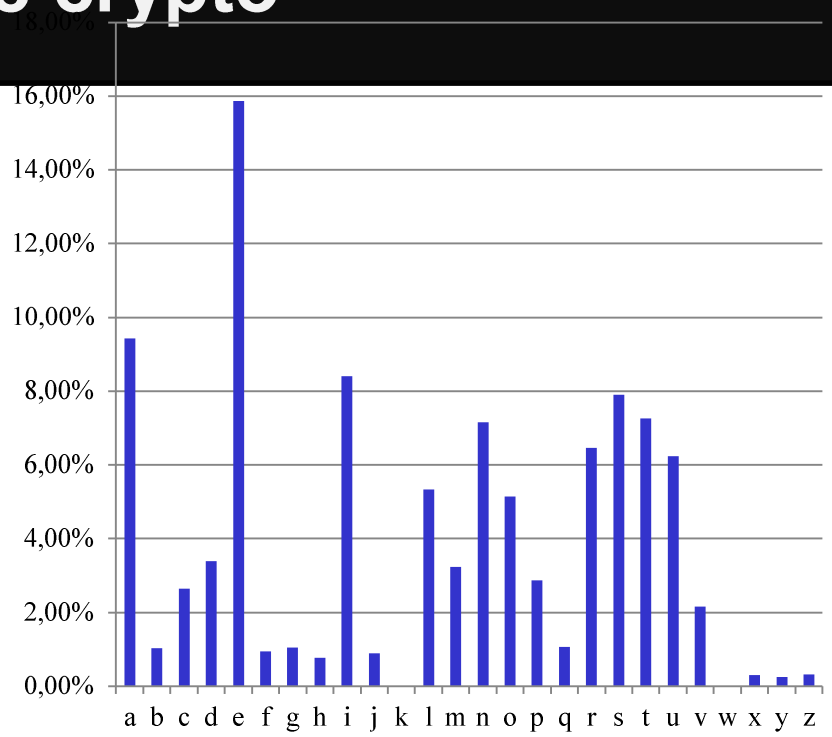
Exercices de crypto

- Réponse question 1 :

  Histogramme des fréquence des lettres du français

  Ci-dessous rangée

  Par fréquence



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

Histogramme ordonné du texte chiffré

(en jaune quand il y a égalité)

Exercices de crypto

- Réponse question 1 (complément) :
  - Possibilité de combiner l'analyse fréquentielle sur les caractères avec l'analyse des digrammes (couples de caractères), les trigrammes, …

Digrammes les plus fréquents en français

Digrammes	Pourcentages
ES	3,15 %
LE	2,46 %
EN	2,42 %
DE	2,15 %
RE	2,09 %
NT	1,97 %

Digrammes les plus fréquents dans le texte

Digrammes	Pourcentages
LE	2,98 %
DE	2,48 %
IS	2,48 %
RT	1,98 %
RE	1,98 %
ES	1,98 %