Mathématiques discrètes
Projet : Mots de passe

Consignes :

Le but du projet est de présenter une application dans laquelle les mathématiques discrètes jouent un rôle fondamental.

Le format du rendu attendu sera celui d'un billet de blog présentant le contexte, puis un apport personnel reposant sur les notions de mathématiques discrètes vues en cours (exercice, quiz, ou programme processing). Une attention particulière doit être apportée à la clarté de la présentation. Celle-ci s'adresse à l'ensemble du groupe donc nécessite un effort de préparation et de pédagogie.

Vos productions seront relues par d'autres étudiants. La note finale prendra en compte la qualité de cette relecture.

Contenu Le sujet détaille quelques points à développer mais ceux-ci sont proposés comme point de départ de votre travail. Vous êtes encouragés à développer d'autres pistes en lien avec les mathématiques discrètes. De même, la bibliographie conseillée est un point de départ. Vous pouvez vous appuyer sur d'autres sources sur lesquelles vous porterez un œil critique et que vous prendrez soin de citer correctement. Vous serez notés sur la compréhension du sujet et le contenu du billet.

Charte de bonne conduite Lisez attentivement la charte de bonne conduite. Portez une attention particulière à citer toutes vos sources, y compris les images que vous utiliserez.

Calendrier Consultez la page Moodle du cours pour les dates des principales étapes du projet.

Bref descriptif du sujet

Les mots de passe sont censés protéger l'accès à nos données, à nos applications,... Les attaques de mots de passes sont nombreuses : par dictionnaire, par force brute. Notre sécurité informatique repose principalement sur le temps de recherche de ce sésame. Le but de ce projet est de comprendre la combinatoire des mots de passe afin de limiter les attaques par force brute.

Bibliographie conseillée

- `https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-forc`
- `http://tomroud.cafe-sciences.org/2011/08/15/entropie-des-mots-de-passe/`
- `https://fr.wikipedia.org/wiki/John_the_Ripper`

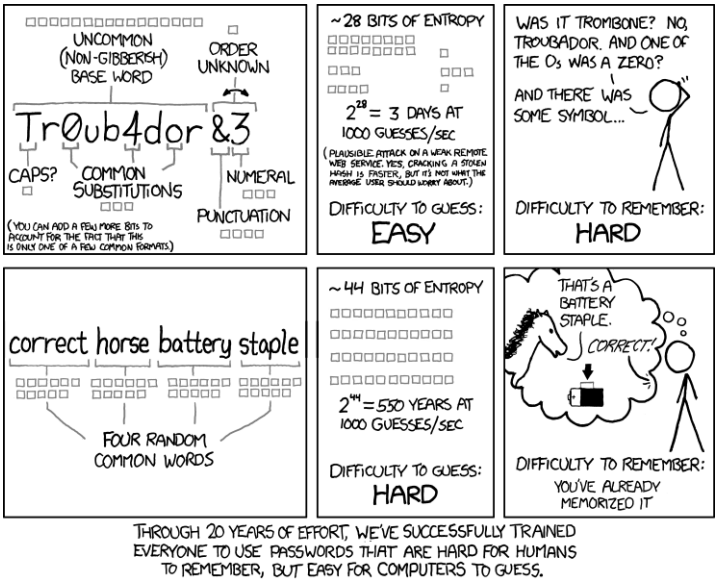

FIGURE 1 – xkcd-936, *a webcomic of romance, sarcasm, math, and language.*

Pistes de développement

1. Expliquer pourquoi on recommande des mots de passe avec au moins 1 majuscule, 1 minuscule, 1 nombre et 1 symbole, d'une longueur d'au moins 12 caractères.
2. Expliquer quel est le problème avec les fonctions de hachage (comme MD5) et le principe du salage
3. Écrire un programme qui étant donné un dictionnaire génère des mots de passe en combinant ces mots et des lettres.
4. Calculer le nombre de mots de passe possible en combinant le jour de naissance, le nom, le prénom. Combien de mots de passe sont possibles si pour allonger le mdp, l'utilisateur répète au moins une fois l'un des éléments ?