Cryptographie

Projets

Partage de secret

Ce projet vous propose de comprendre et d'expérimenter les principes régissants le partage de secret. Vous devrez vous intéresser aussi bien aux principes cryptographiques qu'à leur mise en oeuvre. Pour cela vous devrez rédiger un document présentant de façon précise les principes et techniques que vous envisagez de mettre en oeuvre ainsi qu'un simulateur qui lui sera associé.

Vous étudierez aussi bien le partage de secret simple faisant intervenir l'opérateur $\bigoplus$ que le partage de secret selon Shamir. Vous présenterez également une application de cette idée.

Le rendu sera double (10 janvier 2020 dernier délai) :

- Un rapport de moins de 30 pages décrivant de façon pédagogique les principes cryptographiques qui fondent ces techniques de partage. *(Rmq : Tout plagiat sera sanctionné de la note 00/20)*. A cela s'ajoutera une description précise de l'ensemble des techniques que vous avez mis en oeuvre pour mettre au point votre simulateur.

- Un simulateur permettant de réaliser ce partage de secret. Vous êtes libre des choix techniques. Une démo sera à prévoir le jour du rendu.

sources possibles

- `http://fr.wikipedia.org/`
- ...

Cryptographie
Projets
Chiffre ADFGVX

A l'instar du chiffre ADFGVX, on souhaite mettre en oeuvre un chiffrement basé sur des techniques inspirées du carré de Polybe. Pour cela nous utiliserons un alphabet à 6 symboles qui sera {-, #, +, *, %, .} pour la phase de substitution. Cette substitution se fera par conséquent sur 36 symboles *(les 26 lettres de l'alphabet et les 10 chiffres)* dont la répartition au sein de la grille est laissée à votre discrétion. Elle doit cependant être aléatoire. La phase de transposition sera quant à elle basée sur une clef alphanumérique pouvant faire intervenir ces 36 symboles. Suivant l'ordre alphanumérique, les chiffres sont prioritaires sur les lettres de l'alphabet.

Vous devrez vous intéresser aussi bien aux principes cryptographiques qu'à leur mise en oeuvre. Pour cela vous devrez rédiger un document présentant de façon précise les principes et techniques que vous envisagez de mettre en oeuvre ainsi qu'un simulateur qui lui sera associé pour les opération de chiffrement et de déchiffrement.

La seconde phase du projet consiste en une cryptanalyse des chiffres suivants. Il s'agit de mots anglais. Ils consistent en une substitution faite selon les principes décrits ci-dessus. Afin de vous faciliter la tâche, ils ne sont pas transposés.

- mots anglais
  i) `#++.+%*+#.-%*#%+*+.#*+.*-%`
  ii) `-%%-##*+-%+-*+#.`
  iii) `*%%+.+*.#.+%-.-%%#`
  iv) `-*+*.%*.-*-+.#`
- mots francais
  i) `-%*-%--.**...-..*.%-+-.+`
  ii) `-...#.+*.+*-.+****.+`
  iii) `+*#++++*+%%##+%.#+%*+*`
  iv) `++.%+%%.*#-+#+`

Le rendu sera double (10 janvier 2020 dernier délai) :

- Un rapport de moins de 30 pages décrivant de façon pédagogique l'ensemble des techniques que vous avez mis en oeuvre pour le chiffrement, le déchiffrement et la cryptanalayse. *(Rmq : Tout plagiat sera sanctionné de la note 00/20).*
- Un simulateur permettant de réaliser un chiffrement, un déchiffrement et une cryptanalyse.

sources possibles

- `http://fr.wikipedia.org/wiki/Chiffre_ADFGVX`
- ...

Cryptographie

Projets

Rainbow table

Ce projet consiste à retrouver les mots de passe correspondant à des empreintes MD5 récupérées dans un fichier de mots de passe. On sait que les mots de passe sont construits à partir de mots anglais de 6 lettres auxquels on a mêlé 4 chiffres (exemples : *artist* + *1234* $\longrightarrow$ 1ar23t4ist ; *august* + *9876* $\longrightarrow$ augu987st6 ; ...).

Pour réussir à mener à bien le projet, vous utiliserez une table *arc-en-ciel* (Rainbow table) adaptée à ce format de mots de passe.

Le fichier de mots de passe récupéré contient les lignes suivantes :

```
bb8327c5eabea57fc4139b5cfa32320b
7f828855165aec21e5381420c6eb0e63
332067c895e019aa421375e5a16e3d76
38f63555c94c320a2b605dec864a72cd
93d69b3fee09a2a0159f488043fab008
b56e6c6319ec72927872a928030cf7da
d293ee8d9ebb8c8e4abd8f769b4cd9da
```

Ce qui doit être fourni pour le 9 janvier 2020 dernier délai :

- Un rapport détaillant les principes et algorithmes que vous avez utilisés pour répondre à cette question.
- La table arc-en-ciel et le code original dans le langage de votre choix qui vous a permis de la générer.
- Le fichier des mots de passe déchiffrés.

Cryptographie

Projets

Factorisation d'Entiers

Ce projet vous propose de mener une cryptanalyse (légèrement dégradée) d'un processus cryptographique asymétrique basé sur `RSA`. La tâche qui vous est confiée est la suivante : Le nombre ci-dessous est le produit de deux nombres premiers. C'est l'unique information qui est à votre disposition. L'objectif à atteindre est de retrouver ses 2 facteurs. Pour cela, vous devrez mettre en oeuvre par vous même les outils nécessaires à cette tâche. Vous n'avez pas la possibilité d'utiliser des logiciels tout fait. Vous avez par contre tout le loisir d'utiliser d'éventuelles données disponibles sur Internet ou ailleurs.

Le rendu sera double (10 janvier 2020 dernier délai) :

- Un rapport de moins de 30 pages décrivant en détails la démarche scientifique que vous avez utilisée pour arriver à vos fins. *(Rmq : Tout plagiat sera sanctionné de la note 00/20).*

- Le logiciel de cryptanalyse que vous aurez implanté vous permettant d'arriver au résultat. Une démo sera à prévoir le jour du rendu. Afin d'éprouver votre approche, un autre nombre à factoriser vous sera fourni pour cette démo.

83424792058117331
68604327633318283
739146272243141978647
3653977318573249834539450154490884099169205123 53

sources possibles

- `https://en.wikipedia.org/wiki/Pollard's_rho_algorithm`
- `https://fr.wikipedia.org/wiki/Crible_quadratique`
- `http://thales.doa.fmph.uniba.sk/macaj/skola/teoriapoli/primes.pdf`

Cryptographie

Projets

One Time Password

Le One-time-password est un mot-de-passe à usage unique, c.a.d. il permet l'authentification lors d'une unique session. Ils ont été conçus pour pallier aux attaques par rejeu, car lorsqu'on récupère un mot-de-passe, on ne pourra pas le re-utiliser par ailleurs. Les OTP sont souvent construits à base de plusieurs primitives cryptographiques : les fonctions pseudo-aléatoires et de fonctions difficiles à inverser, e.g. les fonctions de hachage (SHA).

Vous étudierez plusieurs solutions OTP proposées sur la marché (e.g. OTP avec une synchronization en temps, SMS-OTP etc.) et vous ferez également une étude de leur sécurité. On demande à la fois une analyse des outils cryptographiques et des moyens techniques utilisés pour leur mise en œuvre.

Le rendu sera double (10 janvier 2020 dernier délai) :

- Un rapport de moins de 30 pages décrivant en détails la démarche scientifique que vous avez utilisée pour arriver à vos fins. *(Rmq : Tout plagiat sera sanctionné de la note 00/20).*

- Un simulateur type client/serveur permettant l'authentification via un OTP (de préférence basé sur HMAC) sera réalisé. Vous êtes libres des choix techniques. Une démo sera à prévoir le jour du rendu.

sources possibles

- `https://en.wikipedia.org/wiki/One-time_password`
- `https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm`
- `https://en.wikipedia.org/wiki/Message_authentication_code`

sources possibles

- `http://lifehacker.com/five-best-file-encryption-tools-5677725`
- `https://www.openssl.org/`

Cryptographie

Projets

Hashcash- contremesure aux attaques DoS

Hashcash est un système de type preuve de travail, basé sur les fonctions de hachage. Il est utilisé pour limiter les le spam d'email, pour premunir aux attaques type Denial of Service et dans les constructions plus récents de monnaie numérique (e.g. bitcoin). Ce projet vous propose de comprendre et d'expérimenter les principes régissants le Hashcash. Vous devrez vous intéresser aussi bien aux principes cryptographiques qu'à leur mise en oeuvre. Pour cela vous devrez rédiger un document présentant de façon précise les principes et techniques que vous envisagez de mettre en oeuvre ainsi qu'un simulateur qui lui sera associé.

Le rendu sera double (10 janvier 2020 dernier délai) :

- Un rapport de moins de 30 pages décrivant de façon pédagogique les principes cryptographiques qui fondent la sécurité de la monnaie virtuelle `bitcoin`. *(Rmq : Tout plagiat sera sanctionné de la note 00/20)*. La seconde partie de ce rapport sera consacrée à la description de ces principes pour mettre en place une technique de vote électronique. Cette notice explicative trouvera écho dans le simulateur que vous fournirez.

- Un simulateur type client/serveur permettant de réaliser Hashcash. Vous êtes libre des choix techniques. Une démo sera à prévoir le jour du rendu.

sources possibles

- `https://infogalactic.com/info/Hashcash`
- `http://www.hashcash.org/papers/hashcash.pdf`
- `http://pennypost.sourceforge.net/PennyPost`
- `http://mapson.sourceforge.net/`