Notes de cours
Semaine 11

Cours Turing

1 Cryptographie à clé publique

Dans ce chapitre, nous allons voir le protocole d'échange de clé de Diffie-Hellman-Merkle : c'est un protocole astucieux qui permet à Alice et Bob d'échanger une clé secrète en ne faisant qu'échanger des messages qui peuvent être écoutés par tout le monde ! (pour ensuite utiliser cette clé pour communiquer avec un système de cryptographie à clé secrète, comme DES).

Bien sûr, il peut sembler a priori complètement impossible qu'Alice et Bob parviennent à se mettre d'accord sur une clé secrète s'ils ne peuvent qu'échanger des messages dits *publics*, à savoir des messages qu'Eve écoute en permamence. Et dans l'absolu, c'est vrai : c'est impossible...

Mais il se trouve que ça devient possible si on ajoute l'hypothèse qu'Eve n'a pas une puissance de calcul infinie, et qu'Alice et Bob disposent de ce qu'on appelle une *opération à sens unique*, c'est-à-dire une opération qu'il est facile d'effectuer (i.e., qu'il est possible d'effectuer en un temps raisonnable), mais très difficile d'inverser (par *très difficile*, on entend ici que le temps nécessaire pour effectuer cette inversion est beaucoup trop long). Voyons ceci en détail.

1.1 Le protocole d'échange de clé de Diffie-Hellman-Merkle : principe

En guise d'introduction, nous allons d'abord voir une version simplifée de ce protocole. Pour ce faire, nous allons supposer que l'opération à sens unique mentionnée ci-dessus est la multiplication. Vous objecterez qu'il est à l'heure actuelle très facile d'effectuer l'opération inverse, à savoir la division, ce qui est vrai ; mais on peut quand-même dire qu'il est en général plus difficile de diviser que de multiplier. Par extension, imaginons donc un monde où il soit *très difficile* d'effectuer des divisions.

1. Pour commencer, Alice et Bob se mettent d'accord sur un nombre entier commun M, qu'ils communiquent "en clair" à tout le monde (et donc en particulier à Eve, qui écoute tout).
2. Puis Alice choisit en secret un nombre entier A_1 et effectue la multiplication $A_2 = M \cdot A_1$; Bob fait de même de son côté en choisissant un nombre secret B_1 et en effectuant la multiplication $B_2 = M \cdot B_1$.

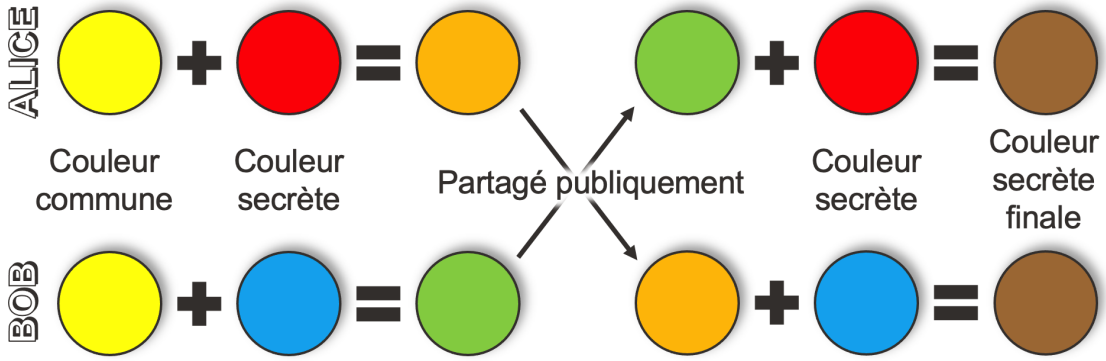
3. Alice communique ensuite le nombre A_2 à Bob, et Bob communique le nombre B_2 à Alice. Eve, qui a tout écouté (pour rappel, Alice et Bob ne peuvent rien communiquer secrètement), a donc maintenant entendu les valeurs des nombres M, A_2 et B_2 .
4. Puis Alice reprend son nombre secret A_1 et effectue, toujours en secret, la multiplication $A_3 = B_2 \cdot A_1$; de même, Bob effectue en secret la multiplication $B_3 = A_2 \cdot B_1$.

Que valent donc A_3 et B_3 ? $A_3 = B_2 \cdot A_1 = M \cdot B_1 \cdot A_1$ et $B_3 = A_2 \cdot B_1 = M \cdot A_1 \cdot B_1$. Vu que la multiplication est commutative, ces deux nombres sont égaux : $K = A_3 = B_3$ est donc la clé secrète partagée entre Alice et Bob.

Bien entendu, il faut encore vérfifier qu'Eve ne puisse pas trouver la clé K. Mais vous pouvez vérifier en effet qu'avec seulement les valeurs de M, A_2 et B_2 à disposition, Eve est incapable de trouver la clé K si elle ne sait pas effectuer des divisions (ou ne peut pas effectuer ces divisions en un temps raisonnable, ce qui revient au même). K est donc bien le secret partagé d'Alice et Bob.

Finalement, il importe d'observer encore une chose : Alice et Bob vivent dans le même monde qu'Eve et ne savent donc pas diviser non plus, par hypothèse. Ceci veut dire que même s'ils ont pu se mettre d'accord sur une clé secrète commune K, ni l'un ni l'autre n'est capable de retrouver le nombre secret initial choisi par l'autre, même à la fin du protocole. Ainsi, Alice ne connaît pas B_1, ni Bob ne connaît A_1. Ces deux nombres restent *privés*, tandis que A_2 et B_2 sont eux *publics*. Et c'est la combinaison de A_1 et B_2 d'une part, et de B_1 et A_2 d'autre part, qui permet de trouver le secret commun K.

Une autre façon encore plus visuelle (voir la figure ci-dessous) d'envisager ce protocole est de penser à des pots de peinture de différentes couleurs (qu'il est facile de mélanger, mais très difficile de séparer). Alice et Bob se mettent d'accord au départ sur une couleur commune (disons le jaune), et choisissent chacun en secret une autre couleur (le rouge pour Alice, le bleu pour Bob). Alice mélange le jaune et le rouge, obtenant ainsi de l'orange, et transmet cette couleur à Bob ; Bob mélange de son côté le jaune et le bleu, obtenant ainsi du vert, et transmet cette couleur à Alice. Puis Bob mélange la couleur reçue d'Alice, l'orange, avec sa couleur secrète, le bleu, et obtient du brun. Alice de son côté mélange le vert reçu de Bob avec sa couleur secrète, le rouge, et obtient le même brun. Mais Eve, qui n'a vu passer que les pots de couleur jaune, orange et vert, n'est pas en mesure d'obtenir le même brun qu'Alice et Bob :



1.2 Fonctions à sens unique

Dans la suite, nous allons parler de *fonctions à sens unique*, plutôt que d'opérations à sens unique. *Grosso modo*[1], une fonction à sens unique est une fonction F telle que :

1. Pour toute valeur de A, il est facile de calculer $F(A)$.
2. Si on nous donne une valeur de B (faisant partie de l'image de F), il est alors très difficile de trouver une valeur de A telle que $F(A) = B$.

Cette deuxième ligne donne une condition plus stricte à respecter que la condition d'être "difficile à inverser". Voyez plutôt :

- La fonction F telle que $F(A) = 0$ pour toute valeur de A est la fonction la plus difficile à inverser qui soit ! Pour autant, ça n'est pas une fonction à sens unique, car il est facile de trouver une valeur de A telle que $F(A) = 0$ (en effet, n'importe quelle valeur de A fonctionne !)

- De même, pour un entier N donné, la fonction $F(A) = A \pmod N$ définie sur tous les nombres entiers A n'est pas à sens unique, car pour une valeur B entre comprise entre 0 et $N - 1$, il suffit de choisir $A = B$ pour trouver $F(A) = B$.

- Par contre, il se trouve que la *fonction de Rabin* $F(A) = A^2 \pmod N$ est une fonction à sens unique si $N = P \cdot Q$, avec P et Q des grands nombres premiers (et qu'on connaît seulement la valeur de N, et pas les facteurs P et Q). C'est sur cette fonction que se base le *cryptosystème de Rabin*, mais celui-ci reste un peu technique à étudier...

Dans la paragraphe suivant, vous découvrirez la fonction à sens unique utilisée dans le protocole de Diffie-Hellman-Merkle.

Pour faire le lien avec ce dont nous avons parlé il y a deux semaines, notez au passage que ces fonctions à sens unique sont non seulement intéressantes pour la cryptographie, mais aussi pour générer des suites de nombres aléatoires !

Le problème du "logarithme discret"

En arithmétique classique, si quelqu'un vous donne les valeurs de deux nombres A et C et vous dit que $A^B = C$, il est facile de calculer la valeur de B en utilisant la formule

$$B = \log_A(C)$$

Bon, il est vrai que calculer un logarithme à la main n'est pas si facile, mais toute calculatrice digne de ce nom vous permettra de faire ça rapidement.

En arithmétique modulaire, rien n'est moins vrai ! En effet, si on nous donne : N un grand nombre premier, A et C deux nombres compris entre 2 et $N - 1$, et qu'on nous dit que $A^B \pmod N = C$, il est alors très difficile de retrouver la valeur de B. On appelle ça le *problème du logarithme discret* (par analogie à la relation trouvée ci-dessus pour la valeur de B dans le cas continu).

1. Notez bien qu'en théorie, on n'est jamais totalement sûr qu'une fonction soit vraiment à sens unique...

Par contre, nous avons vu la dernière fois qu'il est possible d'effectuer rapidement l'exponentiation modulaire $A^B \pmod N$. De ces deux constatations, nous déduisons que la fonction F suivante est une fonction à sens unique :

$$F(B) = A^B \pmod N$$

où N est un grand nombre premier et $2 \leq A \leq N-1$.

1.3 Le vrai protocole de Diffie-Hellman-Merkle

Nous allons maintenant tirer parti de cette fonction à sens unique pour permettre à Alice et Bob de se mettre d'accord sur un secret commun, en supposant qu'Eve n'a pas la puissance de calcul nécessaire pour résoudre le problème du logarithme discret (ce qui est somme toute une hypothèse très réaliste). Voici le protocole :

1. Alice et Bob se mettent d'accord sur la valeur d'un grand nombre premier N, ainsi que sur un autre nombre M compris entre 2 et $N-1$. Eve, qui écoute tout, connaît donc également les valeurs de M et N.
2. Alice choisit secrètement un nombre $2 \leq A_1 < N$ et effectue l'opération $A_2 = M^{A_1} \pmod N$. De son côté, Bob fait la même chose : il choisit $2 \leq B_1 < N$ et effectue $B_2 = M^{B_1} \pmod N$.
3. Alice communique la valeur de A_2 à Bob et Bob communique la valeur de B_2 à Alice. Eve, qui encore une fois écoute tout, apprend donc les valeurs de A_2 et B_2.
4. Alice calcule (de son côté) $A_3 = B_2^{A_1} \pmod N$ et Bob calcule (aussi de son côté) $B_3 = A_2^{B_1} \pmod N$.

Nous allons maintenant vérifier les deux affirmations suivantes :

1. $A_3 = B_3 = K$: Alice et Bob ont donc réussi à se mettre d'accord sur un secret commun.
2. Avec les informations dont elle dispose (et en supposant qu'elle n'a pas une puissance de calcul infinie), Eve ne peut pas deviner la valeur de K, qui sera donc le secret commun d'Alice et de Bob.

En effet, on voit que

$$A_3 = B_2^{A_1} \pmod N = (M^{B_1} \pmod N)^{A_1} \pmod N = (M^{B_1})^{A_1} \pmod N = M^{B_1 \cdot A_1} \pmod N$$
$$B_3 = A_2^{B_1} \pmod N = (M^{A_1} \pmod N)^{B_1} \pmod N = (M^{A_1})^{B_1} \pmod N = M^{A_1 \cdot B_1} \pmod N$$

ce qui confirme le premier point : les valeurs de A_3 et B_3 sont égales (car $B_1 \cdot A_1 = A_1 \cdot B_1$). Quelles sont donc maintenant les informations dont dispose Eve ? Elle connaît :

$$N, \quad M, \quad A_2 = M^{A_1} \pmod N \quad \text{ainsi que} \quad B_2 = M^{B_1} \pmod N$$

A moins d'être capable de résoudre le problème du logarithme discret, Eve ne peut donc pas retrouver les valeurs de A_1 ou B_1, ni pas conséquent la valeur de $A_3 = B_3 = K$: Alice et Bob ont donc bien trouvé un secret commun K, qu'ils peuvent utiliser pour communiquer secrètement grâce au protocole DES, par exemple (rappelez-vous que vu que K est un grand nombre, sa

représentation binaire est une longue suite de bits, certes pas complètement aléatoire, mais c'est un moindre défaut).

A noter que, comme dans l'exemple avec les multiplications et les divisions, les nombres A_1 et B_1 restent secrets tout au long du protocole. Alice et Bob n'ont pas besoin de révéler ces nombres respectifs à leur partenaire ; le protocole fonctionne sans ça.

1.4 Défauts du système

Pour finir, mentionnons que ce système a un défaut principal : c'est justement celui d'être d'un protocole d'échange de clé, qui nécessite après coup l'utilisation d'un système de cryptographie à clé secrète pour échanger des messages. La semaine prochaine, nous verrons d'autres protocoles de cryptographie à clé publique, qui permettent d'échanger directement des messages de manière confidentielle.

L'autre défaut de ce système est celui déjà mentionné plus haut : il n'existe aucune garantie théorique que le problème du logarithme discret soit un problème *vraiment* difficile à résoudre. Qui sait, peut-être que dans quelques années, quelqu'un trouvera un algorithme efficace pour résoudre ce problème ? Ceci remettrait en question bien des choses... En prévision de cela, certaines personnes s'intéressent à de nouveaux systèmes cryptographiques, comme celui évoqué dans le paragraphe suivant.

1.5 Le même protocole avec des courbes elliptiques !

En général, lorsqu'on entend parler de "courbes elliptiques", on pense tout de suite à quelque chose de substantiellement complexe, donc difficile à approcher (par exemple, les courbes elliptiques apparaissent dans la démonstration du grand théorème de Fermat évoqué la semaine dernière). Il se trouve cependant que celles-ci peuvent être utilisées pour une version modifiée du protocole d'échange de clé de Diffie-Hellman-Merkle, et que cette utilisation est très bien expliquée dans l'excellent blog de Fang-Pen Lin (en anglais) :

`https://fangpenlin.com/posts/2019/10/07/elliptic-curve-cryptography-explained/`

Nous éviterons de bêtement paraphraser ce blog dans le présent chapitre, mais nous passerons à travers les idées principales de celui-ci pendant le cours.