Sécurisation des communications

Architecture matérielle, systèmes d'exploitation et réseaux

① La sécurité des communications

Lorsque deux personnes communiquent par l'intermédiaire d'un réseau informatique, elles sont en droit d'exiger que cette communication se déroule de façon sécurisée, autrement dit qu'elle respecte les principes de *confidentialité* (les deux personnes doivent être les seuls à lire leurs messages), d'*intégrité* (le message reçu est identique au message envoyé : il n'a pas été modifié en chemin) et d'*authentification* (chaque personne doit être sûre de bien échanger avec la bonne personne).

L'objet de cette activité est de découvrir différentes méthodes développées pour tenter d'apporter des garanties quant au respect de ces trois principes dans toute communication.

② Le chiffrement symétrique (dit à clé partagée)

2.1 Activité du cadenas

Imaginons que Serge veuille envoyer à Jeanne un message en le mettant dans une boîte.

1. Sachant que cette boîte a besoin de transiter par plusieurs personnes, comment Serge peut-il procéder pour être sûr que le message ne soit lu que par Jeanne ?
2. Quels sont les avantages et les limites d'une telle méthode ?

③ Le chiffrement asymétrique (dit à clé publique)

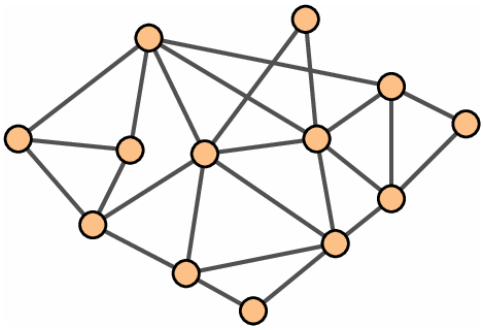
3.1 Adaptation de l'activité du cadenas

On admet que Jeanne et Serge ne peuvent pas se voir pour s'échanger leurs cadenas. Répondre aux questions précédentes en tenant compte de cette nouvelle contrainte.

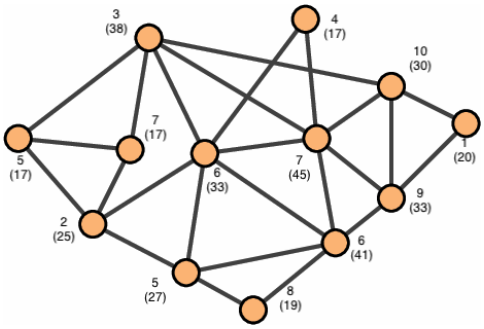
3.2 Activité du graphe

Imaginons maintenant que Jeanne et Serge ne disposent ni de boîtes, ni de cadenas pour les verrouiller. Serge souhaite envoyer un message sécurisé à Jeanne. Dans l'activité qui suit nous allons réduire ce message à un nombre entier positif. Ne disposant pas de boîte sécurisée, il décide de *chiffrer* ce nombre, autrement dit, de le rendre incompréhensible à toute personne ne disposant pas d'une *clé*. Il choisit la méthode de chiffrement asymétrique introduite ci-dessus.

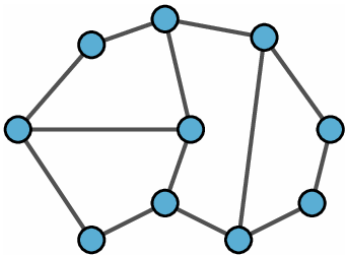
Dans un premier temps, Jeanne présente sa *clé publique* : il s'agit d'un plan simplifié de son quartier (figure ci-dessous). En mathématiques et en informatique, ce plan est appelé un *graphe*. Il est composé de *sommets* (les intersections) et d'*arêtes* (les rues).



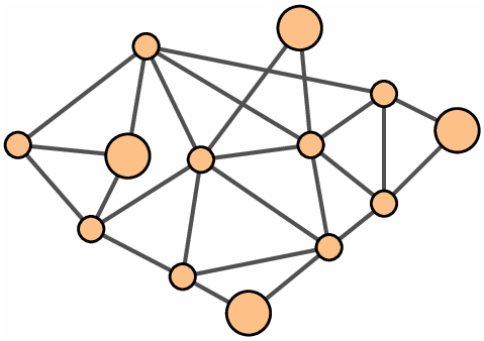
Serge va utiliser cette clé publique de Jeanne pour chiffrer son message, par exemple le nombre 73. Il va commencer par écrire celui-ci comme la somme de treize nombres (ce qui correspond exactement au nombre de sommets du graphe) puis reporter, *au crayon à papier* chacun de ces nombres à côté d'un sommet. À ce stade le message n'est pas encore chiffré dans la mesure où il est très simple de retrouver 73 à partir de tous les nombres écrits sur le graphe. Serge va donc procéder de la manière suivante : il écrit, cette fois-ci entre parenthèses et au stylo, la somme de chaque nombre se situant à côté d'un sommet et de tous les nombres situés au voisinage de celui-ci (c'est-à-dire tous les nombres directement reliés au sommet par une seule arête : les deux sommets sont dits *adjacents*). Il efface alors tous les nombres écrits au crayon à papier. Le message est désormais chiffré.



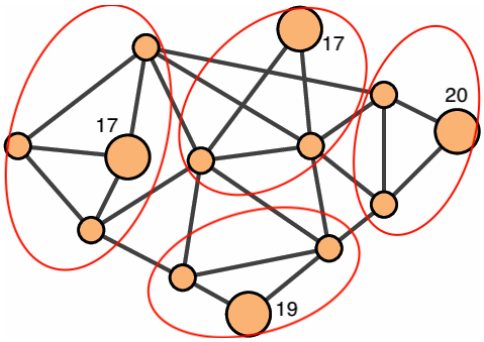
Soit le graphe ci-dessous. Chaque groupe doit chiffrer un nombre de son choix.

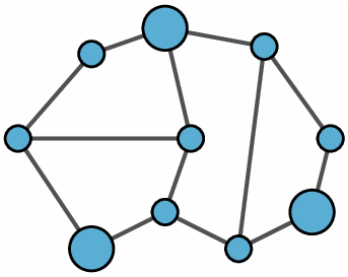


Échangez-vous les graphes et essayez de déchiffrer les messages des autres.



Sur la clé privée, Jeanne a représenté certains sommets avec des points plus larges que les autres. Ils forment ce que l'on appelle un *ensemble dominant parfait* : deux *sommets dominants* ne sont jamais reliés entre eux, et chaque autre sommet est relié directement à exactement un sommet dominant. Ce qui permet, ici, de définir quatre régionnements distincts. *Le nombre à déchiffrer est la somme des nombres situés sur les sommets dominants du graphe* $(17 + 19 + 20 + 17 = 73)$.





S'il n'est pas du tout évident d'exhiber ce type d'ensemble dans un graphe donné, il est, en revanche, très facile de construire un graphe à partir d'un ensemble dominant. Voici comment procéder :

— dessiner un ensemble de sommets et les marquer comme *dominants* ;

— dessiner un autre ensemble de sommets *dominés* ;

— tracer exactement une arête entre chaque sommet dominé et un sommet dominant ;

— ajouter diverses arêtes entre les sommets dominés.

Construire différentes paires de clés et les faire tester par d'autres groupes.

3.3 Principe mathématique

Dans la réalité, ce sont des logiciels qui produisent cette paire de clés. Ils utilisent le plus souvent l'algorithme de chiffrement RSA qui se base sur l'idée suivante : si l'on obtient un nombre entier n comme produit de deux très grands nombres premiers p et q, il est extrêmement difficile de retrouver les valeurs de p et q uniquement avec la donnée du nombre n.

Schématiquement, la clé publique est le couple (n, e) : il suffit pour chiffrer le message. Pour le déchiffrer, il faut la clé privée, un nombre d que l'on ne sait calculer qu'à partir de p et q. La connaissance de n ne permet pas de retrouver les entiers p et q, indispensables pour calculer la clé privée d.

Le chiffrement et le déchiffrement se font au niveau de la couche « application » du modèle TCP/IP. Ainsi, un tiers qui intercepterait le message durant son transport n'a aucun moyen de le lire.

4 Limites du chiffrement asymétrique

4.1 Signature électronique

Avec le chiffrement asymétrique, Jeanne a la garantie que personne n'a pu lire le message qu'elle vient de recevoir mais elle ne peut en aucun cas être certaine que ce message provient bien de Serge dans la mesure où la clé publique est à la disposition de n'importe qui. C'est pour garantir l'identité de l'émetteur du message que la notion de *signature électronique* a été introduite.

À l'aide d'une *fonction de hachage*, Serge peut générer une *empreinte* de son message : il s'agit d'un « condensé » de celui-ci mais qui ne permet pas de retrouver l'original. Puis il chiffre cette empreinte grâce à sa clé privée (qu'il est le seul à posséder). Ainsi, lorsque Jeanne reçoit un message, elle reçoit également l'empreinte de celui-ci, qu'elle déchiffre grâce à la clé publique de Serge. Elle calcule ensuite elle-même l'empreinte du message reçu, avec la même fonction de hachage, et compare les deux empreintes. Si elles sont identiques, elle est certaine que c'est bien Serge qui est l'expéditeur du message (il est le seul à avoir pu chiffrer l'empreinte) et que le message n'a pas été modifié en chemin.

4.2 Certificat électronique

Le recours à une clé publique pose le problème de l'authenticité de l'entité à qui cette clé est censée appartenir. Un tiers pourrait déposer une clé publique au nom d'une autre personne (via un faux site web par exemple) et se faire passer pour celle-ci dans les échanges. On appelle ce procédé *attaque de l'homme du milieu*.

C'est la raison pour laquelle des organismes de confiance, appelés *autorités de certification* (AC), ont pour rôle de garantir l'identité des entités disposant de clés publiques, à travers un mécanisme de vérification exigeant (présence physique, pièces d'identités, signatures de tiers de confiance, etc.). Elles délivrent un *certificat électronique*, qu'elles signent avec leur clé privée, aux entités satisfaisant à ces conditions d'authenticité. L'ensemble formé par ces autorités et les certificats qu'elles délivrent s'appelle une *infrastructure à clés publiques*.

4.3 Échange d'une clé partagée grâce à un chiffrement asymétrique

Nous avons vu dans la première activité que l'un des problèmes du chiffrement symétrique est la sécurisation de l'échange de la clé partagée (on ne peut pas toujours se rencontrer pour l'échanger en main propre !). Ce qui explique le recours fréquent au chiffrement asymétrique. Mais l'inconvénient de ce dernier est qu'il est généralement beaucoup plus lent que son homologue symétrique. Pour des applications où il faut échanger de nombreuses données, il est difficilement utilisable en pratique. On a alors recours à un protocole hybride : on communique par chiffrement symétrique après avoir utilisé le chiffrement asymétrique pour transmettre la clé partagée.

Remarque 1. Modèle simplifié, celui du programme et des sujets de baccalauréat. Avec TLS 1.3, version majoritaire aujourd'hui, la clé de session est calculée de part et d'autre par un échange de Diffie-Hellman et ne circule jamais sur le réseau.

Le principal protocole qui fonctionne sur ce principe est le protocole TLS (anciennement SSL), fréquemment utilisé pour sécuriser par exemple :

— le protocole HTTP (qui prend alors le nom de HTTPS) ;

— les transactions commerciales ou bancaires en ligne ;

— les partages de fichiers ;

— les connexions à une base de données ;

— les connexions distantes à un serveur ;

— les serveurs de messagerie ;

— les transferts de fichiers via le service FTP ;

— les plates-formes dont les données sont stockées dans le *cloud*.

Un autre protocole répandu est le protocole PGP qui permet, quant à lui, de sécuriser la communication par emails.