Architectures PKI et communications sécurisées

Architectures PKI et communications sécurisées

Jean-Guillaume Dumas
Professeur à l'université de Grenoble-Alpes

Pascal Lafourcade
Professeur sur contrat à l'université d'Auvergne, HDR
Chaire industrielle sur la confiance numérique

Patrick Redon
Expert en cybersécurité dans le secteur de la Défense
et de la protection des infrastructures critiques

Préface de Guillaume Poupard
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information

DUNOD

Toutes les marques citées dans cet ouvrage
sont des marques déposées par leurs propriétaires respectifs.

Illustration de couverture : © iStock.com/Danil Melekhin

5 rue Laromiguière, 75005 Paris
www.dunod.com

ISBN 978-2-10-072615-8

Préface

Corollaire indispensable au fantastique développement du numérique, la sécurité des systèmes d'information est passée en quelques années du rang d'une discipline confidentielle, portée par des domaines d'expertise tels que la cryptologie, à un sujet majeur dont les médias se font l'écho au rythme des attaques informatiques qui ne laissent pas d'inquiéter par leur impact toujours plus grand. L'informatique est partout, là où nous nous y sommes habitués, là où elle est bien visible, mais également enfouie dans la plupart des systèmes industriels. Ce que certains qualifient déjà de quatrième révolution industrielle est une source formidable de gains de productivité, de compétitivité, d'innovation mais les faiblesses induites sont, si nous n'y prenons pas garde, particulièrement préoccupantes.

Ces dernières années ont vu se développer les attaques portées par une cybercriminalité en plein essor. Les escroqueries numériques en tout genre sont devenues une activité particulièrement lucrative et, objectivement, peu risquée pour le moment. Les atteintes à l'image numérique, notamment au travers du « défacement » de sites Internet, sont devenues courantes. Plus graves encore, bien que beaucoup plus discrètes par essence, les intrusions dans les systèmes d'information à des fins de renseignement sont une véritable calamité pour l'économie, mais également pour la protection des données à caractère personnel. Les attaquants sont toujours plus compétents, mieux organisés, plus spécialisés et il est bien difficile de dresser un bilan fiable des conséquences catastrophiques de cette perte d'information stratégique. Enfin, bien qu'heureusement encore rare, le risque majeur des années à venir est le sabotage pur et simple des systèmes au moyen de cyberattaques. La technologie le permet, les motivations sont là, le pire est à venir si nous n'y prenons pas garde collectivement.

Face à ce constat réaliste bien qu'anxiogène, les solutions existent et sont abordables. Il convient tout d'abord de faire face, de ne pas nier le risque. Il faut ensuite accepter de conduire une véritable analyse de la menace : que faut-il protéger, contre quoi, à quel niveau. Enfin, la sécurité doit être intégrée au plus profond de nos systèmes selon trois axes majeurs : la protection, la défense et l'humain. La protection tout d'abord : les systèmes d'information doivent être conçus en tenant compte de principes de sécurité informatique dès leur conception. La sécurité influence l'architecture même des réseaux qui doivent être segmentés et interconnectés en positionnant les bonnes barrières aux bons endroits. La défense ensuite : quelle que soit la qualité des mécanismes de protection, il faut toujours considérer qu'un attaquant, qui peut d'ailleurs être interne à l'organisation, peut réussir à les contourner. Être capable de détecter au plus tôt de telles attaques pour réagir efficacement est indispensable afin

de fortement limiter les conséquences. L'humain enfin : ce facteur est trop souvent négligé dans le cadre d'une approche trop technique des questions de sécurité. L'homme fait partie intégrante des systèmes d'information et, s'il n'est pas formé de manière adaptée, il peut rapidement en être le maillon faible.
Afin d'implémenter cette doctrine, la tâche est immense et nécessite une collaboration de l'ensemble des acteurs qu'ils soient publics ou privés, experts en sécurité ou utilisateurs. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information est l'autorité nationale de défense et de sécurité. Elle coordonne l'action des différents ministères et développe un écosystème à même de proposer des solutions de sécurité pour protéger au juste niveau les systèmes informatiques. Sans passer en revue les nombreux axes de développement, citons cependant la démarche de qualification qui vise à évaluer les produits ainsi que les prestataires de services de sécurité de manière à proposer à ceux qui veulent se défendre des solutions à la fois efficaces et de confiance, deux notions bien distinctes.

Mais la sécurité des systèmes d'information, ce n'est pas seulement une froide discipline technologique indispensable dans un contexte de plus en plus hostile ; c'est avant tout un domaine absolument passionnant, fruit de la rencontre entre de nombreuses disciplines scientifiques et humaines.
Alors étudiant, j'ai découvert ce sujet par hasard, au détour d'un exercice d'algèbre introduisant le concept de cryptographie asymétrique avec le fameux RSA. Ce principe m'a fasciné et, lorsqu'il m'a été permis de faire une thèse de doctorat, je me suis orienté vers la cryptographie asymétrique, une discipline où la théorie et la pratique se rejoignent si naturellement.
Cet ouvrage vous propose un voyage dans les arcanes d'une discipline qui sous-tend la sécurité de la majorité de nos systèmes d'information, une discipline complexe, subtile, difficile à implémenter, mais dont la maîtrise est indispensable à ceux qui veulent vraiment comprendre comment la cybersécurité moderne peut apporter des réponses efficaces à des problèmes d'apparence pourtant insolubles.
Bonne lecture !

Guillaume POUPARD
Directeur général de l'Agence Nationale
de la Sécurité des Systèmes d'Information (ANSSI)

Table des matières

Avant-propos

« *La nécessité est mère de l'invention.* »
Platon (428-348 av. J.-C.),
La République, II

Ce livre s'adresse aux étudiants en master en sécurité ou en informatique, aux enseignants, chercheurs et ingénieurs en sécurité désireux de comprendre ou d'approfondir leurs connaissances des infrastructures de gestion de clefs (PKI).
Il est le résultat de la collaboration des mondes universitaires et industriels et de nombreuses années d'enseignement dans les cours de masters liés à la sécurité de Grenoble (master SCCI, master en apprentissage SAFE) dans lesquels les auteurs ont le plaisir d'enseigner.
Son objectif est de fournir une approche compréhensible des techniques, technologies et enjeux liés à ces infrastructures, leurs mises en œuvre, ainsi que les services et protocoles associés.
Plus d'une centaine de figures accompagnent la lecture des chapitres et chaque chapitre inclut des exercices pour aider le lecteur dans l'assimilation et l'approfondissement des concepts. Cet ouvrage est aussi structuré de manière à ce que chaque chapitre puisse être lu séparément, en veillant à définir l'ensemble des termes utilisés. De plus, les prérequis nécessaires à sa compréhension sont rappelés.

But de l'ouvrage

Le livre est organisé de manière à donner un aperçu général de tout ce qui concerne la cryptographie à clef publique et plus particulièrement des infrastructures de gestion de clefs (IGC, ou « *Public Key Infrastructure* », PKI) nécessaires à la mise en œuvre de cette cryptographie. Il présente ensuite un panorama des techniques et protocoles permettant de réaliser des communications sûres, de X.509 à Bitcoin. Il est organisé autour de quatre principaux axes :

– Une présentation des principaux standards d'architectures : « *PKI for X.509 certificates* » (PKIX), « *Pretty Good Privacy* » (PGP) et les architectures reposant sur l'identité. PKIX est le type d'architecture aujourd'hui le plus largement déployé pour un usage professionnel au quotidien. Son architecture centralisée permet de l'enrichir de services et de soutiens au déploiement, apportant ainsi un usage relativement transparent pour les utilisateurs. Différemment, PGP est très utilisé pour

des usages décentralisés où la confiance s'acquiert par des moyens externes à la « *Public Key Infrastructure* » (PKI).
- Un point de vue pratique complémentaire aux aspects théoriques : tout d'abord par des tutoriels détaillant la mise en œuvre d'outils librement disponibles tels GPG ou OpenSSL et, ensuite, par un exposé des problématiques de déploiement industriel d'infrastructures. En particulier, que l'infrastructure soit à destination d'utilisateurs externes ou internes à l'entreprise mettant en œuvre la PKI, elle est nécessairement accompagnée de documents et procédures décrivant d'une part l'architecture et les moyens mis en œuvre dans la PKI et d'autre part les moyens organisationnels nécessaires à la bonne marche de la PKI.
- Un point de vue de mise en œuvre dans la sécurisation des communications : c'est-à-dire par un exposé de l'utilisation des PKI dans la sécurisation des échanges et des différentes couches réseaux ou applicatives nécessaires aux communications sur Internet : de IPSec, SSL/TLS, HTTPS, DNSSec pour le réseau, à S/MIME, monkeysphere et OTR pour la messagerie électronique, du fonctionnement des cartes bancaires, à SET ou Bitcoin pour les transactions.
- Enfin, le livre traite des normes et de la réglementation en sécurité associées à l'emploi et à la mise en œuvre d'une PKI, tels les Critères Communs, le FIPS-140 ou encore le Référentiel Général de Sécurité émis par l'Agence Nationale de la Sécurité des Systèmes d'Information.

Organisation

Le chapitre 1 présente le problème principal résolu par les architectures à clefs publiques, à savoir l'échange de clefs, ainsi que les insuffisances des échanges de clefs classiques que sont le protocole de Diffie-Hellman et le système Kerberos. Comme dans toute étude de cryptologie, l'étude de l'histoire est fondamentale car elle permet de connaître l'historique des attaques ainsi que l'intérêt et le principe des contre-mesures. Le chapitre 2 pose ensuite les fondations techniques indispensables à une architecture : les annuaires et les signatures électroniques. Ce chapitre présente également les notations et standards classiques du domaine. Le lecteur averti pourra utiliser ce chapitre tout au long de sa lecture. Le chapitre 3 introduit les fondements de la gestion de clefs et des certificats électroniques. Trois organisations générales d'une architecture asymétrique sont ensuite présentées.
Un premier type d'organisation possible, qui est hiérarchique, est décrite en détail aux chapitres 4, 5 et 6. C'est la plus répandue et la plus adaptée par exemple aux entreprises commerciales. Plus précisément, le chapitre 4 décrit le standard PKIX, le chapitre 5, les méthodes de certifications croisées et de confiance distribuée et le chapitre 6 présente les mécanismes de confiance pour le modèle embarqué, dans les systèmes d'exploitation et les navigateurs Internet. Le deuxième type d'organisation possible est une organisation pair-à-pair sans autorité centrale, dont l'archétype est le système PGP qui est détaillé au chapitre 7. Dans le chapitre 8 sont présentées des architectures moins répandues qui permettent, comme dans le cas de Spooky, de généraliser le concept d'attribution de clefs à l'attribution de permissions ou encore d'utiliser l'identité des personnes comme clef publique. Ce chapitre clot la première partie du livre, sur les principes des architectures.

La deuxième partie aborde les aspects pratiques comme le déploiement et l'évaluation de la sécurité. Les chapitres 9 et 10 exposent comment définir une politique de sécurité, déployer sa propre architecture et donnent des exemples d'outils permettant de mettre en place une PKI pour les principaux types d'organisation et de systèmes d'exploitation. Le chapitre 11 donne les standards de base sécurisés par une PKI pour l'authentification, le transport et l'échange de clef.

Le cœur de la deuxième partie se trouve au chapitre 12 qui montre les mécanismes techniques mis en place pour la sécurisation des communications du Web en utilisant les PKI. Il brosse ainsi un panorama de la sécurité Internet, des couches réseaux aux paiements en ligne, en passant par les mails chiffrés.

Enfin, le chapitre 13 explique comment les PKI permettent de faire de la certification et présente le cadre réglementaire français associé.

Pour clarifier l'utilité et la lecture possible de ces différents chapitres, la figure 1 les représente avec leurs dépendances et la figure 2 illustre les différents protocoles étudiés dans la suite du livre et leurs interactions avec différents acteurs majeurs de la confiance numérique.

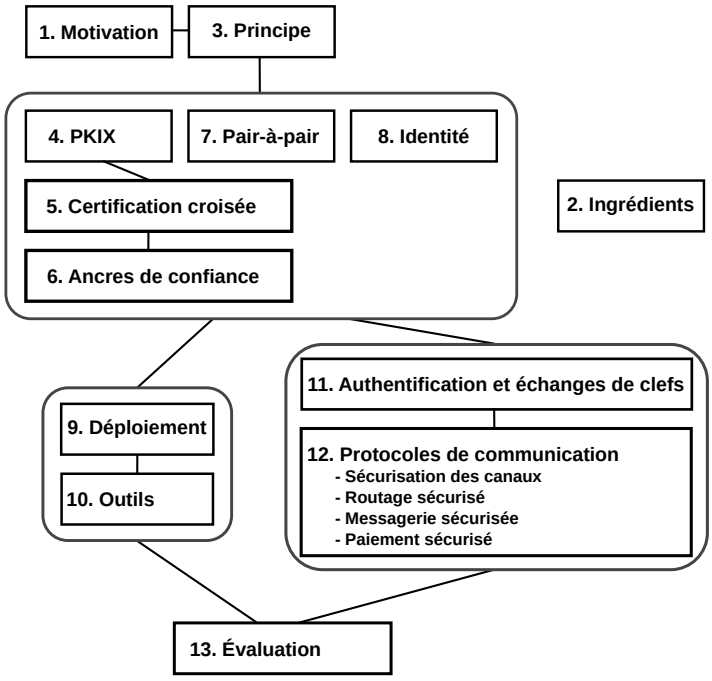

FIGURE 1 – Schéma des dépendances entre les chapitres du livre.

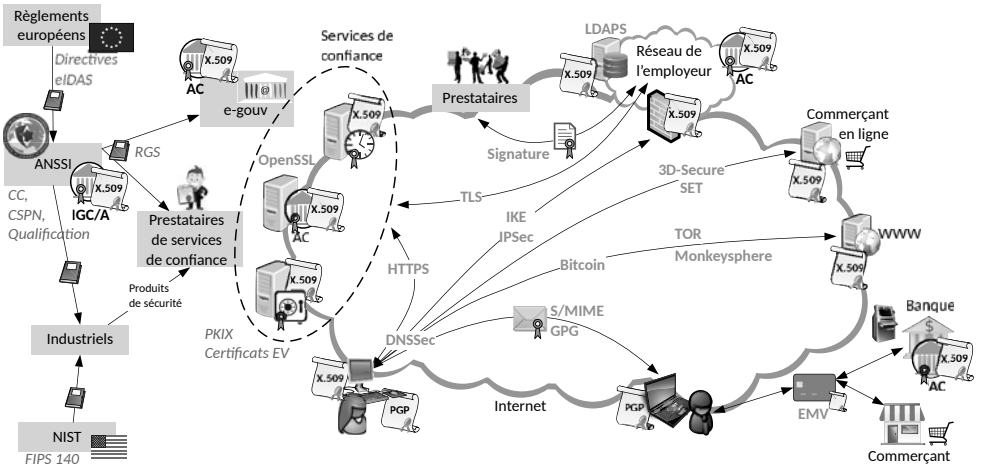

FIGURE 2 – Principaux protocoles étudiés dans *Architectures PKI et communications sécurisées.*

Remerciements

Les auteurs remercient l'ANSSI, le CNES, OpenTrust et Thales d'avoir accepté la reproduction de documents et d'images. Par ailleurs, de nombreuses images utilisées dans les illustrations proviennent du site openclipart.org.
Un grand merci également à Brice BOYER, Dominique DUVAL et Sébastien VARRETTE, ainsi qu'à Laurent FOUSSE et son serveur Git, pour leurs contributions à l'élaboration du contenu de ce livre.
Merci aussi à Joshva BELLAMINE, Christophe BLAD, Jérôme CLERY, Jean-Marie COLLEU, Thierry HASSON, Vladimir KSINANT, Bruno RICCI et Valérie ZORZI pour leurs retours d'expérience sur la mise en œuvre des infrastructures de gestion de clefs et sur la réglementation, permettant d'enrichir le livre avec une vision pratique.
Enfin les auteurs expriment leur gratitude à Floriance ALIXE, Maud BILLETTE, Guénaëlle DE JULIS, David DELON, William DURAND et Jean-Baptiste ORFILA pour leurs commentaires et suggestions de modifications constructifs, suite à leurs relectures assidues.

Grenoble, Aubière, Nantes, le 13 mars 2015.
Jean-Guillaume DUMAS, Pascal LAFOURCADE, Patrick REDON.

Introduction

L'échange d'informations *sensibles* est une problématique intemporelle. Ces informations peuvent être à caractère confidentiel ou nécessiter d'être authentifiées. Indépendamment du support et des moyens d'échanges de ces informations, il est nécessaire d'assurer leur sécurité. Dans le monde réel, les exemples de telles informations sont nombreux. Dans un contrat, la signature, les paraphes et la conservation d'une copie par les parties garantissent l'authenticité et l'intégrité de son contenu. De plus, les informations à caractères personnels transmises à un avocat, à un notaire ou à une administration sont des informations confidentielles, tout comme des données militaires stratégiques.

L'informatique et la dématérialisation ont apporté un média supplémentaire aux échanges. L'essor du réseau Internet et les innovations technologiques entraînent une évolution dans les modes de communication et de consommation. Ordinateurs, téléphones mobiles, tablettes, objets communicants, etc. sont omniprésents. Il est désormais possible, à tout moment, de faire des achats dans une boutique virtuelle, de jouer ou de discuter avec une personne située partout dans le monde, ou encore d'envoyer des documents électroniques. Les échanges sous-jacents à ces services sont gérés par des protocoles de communication complexes que l'utilisateur ne contrôle pas ou très peu alors même qu'ils peuvent nécessiter l'envoi sur le réseau d'informations sensibles ou à caractère personnel, telles un numéro de compte ou de carte bancaire. Les moyens techniques garantissant la sécurité de ces échanges reposent sur la cryptographie. Jusqu'à récemment, la protection des informations ne tenait principalement compte que de la confidentialité, et seule la cryptographie symétrique, utilisant des clef secrètes partagées, était employée. Parmi les exemples connus, il y a le code de César, le code de Vigenère et la machine ENIGMA. Les quarante dernières années ont vu émerger l'étude de nouvelles tendances ajoutant les protections en intégrité et authenticité, cette dernière devenant aussi importante que la protection en confidentialité. Ceci est particulièrement vrai dans le commerce électronique. Dans ce domaine, il faut par exemple pouvoir prouver que la commande vient bien de la personne à qui la livraison est destinée, certifier des actes authentiques comme des contrats.

L'authentification est le mécanisme de validation de l'identité d'une personne ou d'une entité : authentifier c'est être capable de relier de manière certaine une identité et un identifiant connu. Pour cela des chiffrements asymétriques avec des clefs secrètes pour déchiffrer ou signer (des clefs privées) et des identifiants publics pour chiffrer ou vérifier la signature (les clefs publiques) sont utilisés. L'accès aux identifiants et données d'authentification des participants aux échanges est fait grâce à des annuaires élec-

troniques à authenticité garantie. Dans ces annuaires, pierre angulaire des solutions de sécurité présentées dans cet ouvrage, des certificats électroniques permettent de retrouver effectivement les identifiants d'une personne donnée.

Cette authentification est de nos jours omniprésente, tout en étant transparente pour les utilisateurs. Citons par exemple le système EMV (Europay, Mastercard, Visa) sécurisant les transactions embarquées. Une infrastructure à clefs publiques/privées permet aux cartes de s'authentifier auprès des distributeurs de billets par exemple et la garantie d'identité est donnée par une communication avec la banque et/ou le groupement d'intérêt économique. Un autre exemple est le protocole HTTPS qui permet à un site Internet de s'authentifier auprès de notre navigateur afin d'éviter les attaques par hameçonnage (le « *phishing* ») où un site Internet escroc essaie de se faire passer pour un autre afin de récupérer des informations confidentielles. Là encore une architecture à clefs publiques/privées garantit l'identité des sites Internet (il suffit par exemple de cliquer sur le cadenas situé à côté de l'adresse sécurisée par HTTPS pour obtenir des informations sur les organismes, ou entreprises, spécialisés dans les architectures à clefs publiques et qui garantissent l'identité du site en question).

Compte tenu de la croissance du nombre d'objets connectés dans notre vie courante, mais également de l'augmentation des cyber-attaques, la sécurité des communications est devenue une nécessité. Le présent ouvrage décrit les principales solutions déployées aujourd'hui, avec leurs forces, leurs faiblesses et leurs défauts. Le monde est à l'aube de la troisième évolution de l'Internet qui après le Web social doit combiner le Web sémantique avec le Web des objets. Il est toujours difficile de prévoir ou de prédire, une chose est cependant acquise, cette évolution ne se fera pas sans sécurité.

Les codes secrets dans l'histoire

Au cours des siècles, de nombreuses techniques furent élaborées pour protéger les échanges d'informations. Dès l'Antiquité des moyens de transmission d'informations « sûrs » furent développés. Au V^{ième} siècle avant J.-C., Histaïaeus écrivit à Aristagoras en tatouant son message sur le crâne rasé d'un esclave. Il attendit la repousse des cheveux avant d'envoyer le messager demander de l'aide à Aristagoras pour se soulever contre le roi des Perses. Ce procédé s'apparente à la technique dite de *stéganographie*, du grec « *steganos* » signifiant couvert et « *graphein* » signifiant écrire. Cette technique est l'art de cacher un message, de sorte que l'existence même du secret en soit dissimulée. Détecter le message puis le comprendre devient alors difficile sans savoir où et comment chercher. De nombreuses techniques de stéganographie furent inventées comme l'encre invisible au temps de Pline (I^{er} siècle avant J.-C.) ou encore récemment le « *watermarking* » (filigrane électronique) qui permet de dissimuler le copyright d'une image sans qu'il apparaisse sur l'image.

D'autres techniques pour sécuriser les communications furent développées, elles reposent pour la plupart sur une approche cryptographique (du grec « *kruptos* » signifiant cacher et de « *graphein* » signifiant écrire). Les techniques cryptographiques, contrairement à la stéganographie utilisée par Histaïaeus, modifient les messages originaux pour les rendre « incompréhensibles » afin d'assurer un certain niveau de sécurité face aux attaquants. Ainsi, le secret à protéger dans la stéganographie est l'existence

du message, alors que dans une approche cryptographique le secret réside dans les clefs de déchiffrement du message inintelligible.

Une des premières techniques cryptographiques est le chiffrement par transposition, dans laquelle l'ordre des lettres du message original est permuté. Pour déchiffrer le message, il suffit d'appliquer la méthode inverse. Un exemple connu d'un tel chiffrement est la *scytale spartiate*, utilisée au V$^{\text{ième}}$ siècle avant J.-C. par les Grecs. Elle consiste en un bâton, autour duquel est enroulée une lanière de cuir. L'expéditeur écrit son message sur la lanière, puis une fois terminé la déroule et l'envoie. Le récepteur enroule à son tour la lanière reçue sur un bâton de même diamètre, ce qui lui permet ainsi de retrouver le texte original. Dans cet exemple, le diamètre du bâton est secret et permet de protéger l'information.

Une autre technique, appelée chiffrement par substitution, consiste à changer l'alphabet pour chiffrer un message. Elle était déjà utilisée du temps des Romains sous le nom de *chiffrement de César*. Le chiffrement du message est réalisé en décalant de trois lettres dans l'alphabet chaque lettre du message à transmettre. Pour décoder un message chiffré, il suffit de décaler chacune des lettres de trois positions dans le sens inverse de l'alphabet. Dans cet exemple, ce qui devient secret et permet de protéger l'information est la liste des décalages à effectuer dans l'alphabet. Notons que, dans une langue donnée, une étude des fréquences d'apparition des lettres de l'alphabet dans un texte fournit une aide précieuse pour « casser » les chiffrements par substitution. Possédant un texte d'une longueur suffisante, il est alors possible de deviner les lettres les plus usitées, et ainsi de déchiffrer le message. Le chiffrement de Vigenère (XVI$^{\text{ième}}$ siècle) est un autre chiffrement par substitution, plus évolué : plusieurs chiffrements par substitution sont appliqués dans un certain ordre. Cet ordre correspond à un mot ou une phrase connu de l'expéditeur et du récepteur du message. Cette information partagée constitue une *clef* qui permet d'effectuer dans le bon ordre les différents chiffrements par substitution. Le chiffrement de Vigenère est lui aussi sensible à l'analyse de fréquence lorsque la clef est de taille fixée. Au contraire, si la clef est aussi longue que le message à chiffrer, il s'agit du chiffrement symétrique parfait aussi appelé *chiffrement à masque jetable* (« *One-time Pad* ») qui sera présenté un peu plus loin.

Pour terminer, citons un dernier exemple historique. Entre les deux guerres mondiales, les Allemands mirent au point la machine ENIGMA. Celle-ci permettait de chiffrer un message grâce à un dispositif électromécanique qui, en fonction d'une clef donnée, réalisait une certaine combinaison de substitutions polyalphabétiques et de transpositions. Ainsi les Allemands pensaient communiquer des informations en toute sécurité à leurs troupes. Mais les Alliés, sous la direction d'Alan Turing, mirent au point LA BOMBE, un des premiers ordinateurs. Ceci a permis de déchiffrer les messages générés par ENIGMA. Pour plus de précisions sur ENIGMA et les codes secrets dans l'Histoire, le lecteur peut consulter le célèbre livre de S. Singh [Sin99].

Les méthodes cryptographiques présentées utilisent un algorithme et une clef secrète, cette dernière ne devant être connue que des seuls participants à l'échange. La transmission de cette clef qui s'effectuait, il y a encore quelques années, par un échange physique entre personnes de confiance, constitue une étape primordiale dans le protocole de communication. La confidentialité de l'échange reposant sur cette clef, sa connaissance par un tiers réduit à néant la protection apportée.

Objectifs de sécurité

L'objectif fondamental de la cryptographie est de permettre à deux personnes, appelées traditionnellement *Alice* et *Bob* de communiquer à travers un canal peu sûr de telle sorte qu'un opposant, *Oscar*, qui a accès aux informations qui circulent sur le canal de communication, ne puisse ni comprendre et/ou modifier ce qui est échangé, ni se faire passe pour Alice ou Bob. Le canal peut être par exemple une ligne téléphonique ou tout autre réseau de communication.
Les communications échangées entre Alice et Bob sont sujettes à un certain nombre de menaces. La cryptographie apporte des fonctionnalités permettant de répondre à ces menaces, résumées dans l'ensemble Confidentialité, Authentification, Intégrité, Non-répudiation (CAIN) :

Confidentialité des informations stockées ou manipulées par le biais des algorithmes de chiffrement. La confidentialité consiste à garantir que seules ont accès aux informations les personnes autorisées à les connaître ou, en d'autres termes, à *empêcher l'accès* aux informations à ceux qui n'en sont pas les destinataires. Ils peuvent lire les messages chiffrés transmis sur le canal mais ne doivent pas pouvoir accéder à leurs contenus.

Authentification des protagonistes d'une communication. L'authentification a pour but de valider l'identité d'une personne ou bien de détecter une usurpation d'identité, afin d'avoir la garantie que la personne est bien celle qu'elle prétend être. Le terme « authentification » est également utilisé pour désigner la vérification de l'origine de données reçues (aussi appelée « preuve d'origine »). Par exemple, Alice peut s'authentifier en prouvant à Bob qu'elle connaît un secret S qu'elle est la seule à pouvoir connaître.

Intégrité des informations stockées ou manipulées. L'intégrité a pour but de vérifier que le message n'a pas subi d'*altérations* lors de son parcours (cf. figure 3). Cette vérification concerne par exemple une potentielle modification ou substitution volontaire et malicieuse de l'information provoquée par un tiers lors du transfert sur un canal de communication. Ces modifications sont en général masquées par le tiers pour être difficilement détectables. Sur la figure 3, par exemple, le contrôle d'intégrité sur un message M se fait grâce à une fonction f telle qu'il doit être très difficile de trouver deux messages M_1 et M_2 ayant la même image A par f.

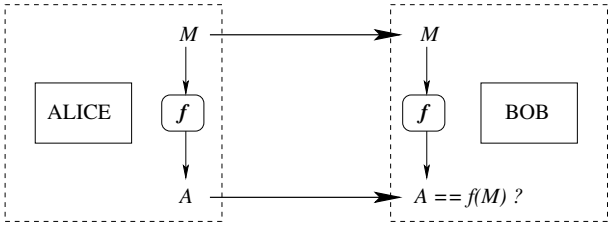

FIGURE 3 – Principe d'un algorithme de contrôle d'intégrité.

Non-répudiation des informations. C'est une protection entre les protagonistes d'un échange, et non plus contre un tiers. Si Alice envoie un message M, elle ne doit pas pouvoir prétendre ensuite devant Bob qu'elle ne l'a pas fait, ou alors qu'elle a envoyé M' et que le message a été mal compris et réciproquement. Techniquement, il s'agit souvent d'une combinaison d'authentification et d'intégrité prouvable à un tiers, par exemple un magistrat. C'est pour cela que des algorithmes asymétriques sont aujourd'hui indispensables.

Ces quatre services sont les principales propriétés de sécurité nécessaires dans les communications sécurisées mais elles ne sont pas les seules ; il y a par exemple :

Le contrôle d'accès qui est la faculté de limiter et de contrôler l'utilisation de systèmes ou d'applications via des maillons de communication. Il est en général nécessaire de s'authentifier ou d'être authentifié au préalable, et les droits d'accès sont alors adaptés en conséquence.

La disponibilité des ressources. Une attaque classique des systèmes est le déni de service qui implique une perte ou une réduction de l'accès à ces ressources. Cela nécessite donc des contre-mesures, soit automatiques, soit par action humaine, afin de prévenir la perte de disponibilité ou de rétablir l'accessibilité.

La fraîcheur des messages. Cette propriété assure que les messages viennent d'être fraîchement générés et ainsi d'éviter les attaques dites « *par rejeu* ». En effet une attaque aisée sur des systèmes d'information consiste à rejouer tout ou partie d'une communication préalablement enregistrée. Se prémunir contre le rejeu de message est un mécanisme qui peut s'effectuer simplement par l'ajout de compteur ou encore de nonces (« *Number used ONCE* »). Il n'est pas rare que ces mécanismes permettent par la même occasion d'authentifier les participants (par exemple dans TLS ou IPSec présentés dans le chapitre 12).

Jusqu'à une période récente, le chiffrement ne tenait compte que de la confidentialité, et seules les méthodes à clefs secrètes étaient développées. Les quarante dernières années ont vu émerger l'étude de nouvelles tendances :

– l'authentification devient aussi, voire plus, importante que le secret. C'est particulièrement vrai dans le commerce électronique : il faut pouvoir prouver que la commande vient bien de la personne à qui la livraison est destinée pour éviter les contestations ;
– une partie de la clef doit être publique, afin de ne pas provoquer une explosion du nombre de clefs nécessaires pour communiquer avec un grand nombre de personnes. Les termes de paire de clefs publique/privée ou encore de bi-clef sont souvent utilisés.

Un dernier critère primordial est l'efficacité des calculs de chiffrement et déchiffrement, de par la taille des messages chiffrés. Les opérations portant sur de grandes quantités de données, le critère d'efficacité est très important afin de pouvoir chiffrer « à la volée » des flux audio ou vidéo par exemple en utilisant au minimum la bande passante. Un système de chiffrement idéal devrait résoudre tous ces problèmes simultanément : utiliser des clefs publiques, assurer le secret, l'authentification et l'intégrité, le tout le plus rapidement possible, tout en garantissant la non-répudiation. Malheureusement, il n'existe pas encore de technique unique qui satisfasse tous ces critères. Les systèmes conventionnels comme « *Advanced Encryption Standard* » (AES) sont efficaces mais

utilisent des clefs secrètes ; les systèmes à clef publique peuvent assurer l'authentification mais sont inefficaces pour le chiffrement de grandes quantités de données car trop coûteux. Cette complémentarité a motivé le développement de protocoles cryptographiques hybrides, à l'instar de *PGP* (cf. chapitre 7), qui utilisent à la fois des paires de clefs publique/privée et des clefs secrètes.

Un peu de cryptographie

La cryptographie est un ensemble de techniques qui protègent un message en le transformant en un autre message : cette transformation modifie l'information contenue dans le message original pour rendre l'information transmise non compréhensible. Parallèlement à la mise en œuvre de méthodes cryptographiques, des méthodes de cryptanalyse ont vu le jour pour intercepter les messages. Ainsi, les cryptographes inventent des méthodes de chiffrement de plus en plus complexes, composées d'une fonction de chiffrement et d'une fonction de déchiffrement. La fonction de *chiffrement* permet de chiffrer un message donné m à l'aide d'une *clef* k, paramètre de la fonction de chiffrement. La fonction est notée E_k. Le message m chiffré par la clef k est noté $E_k(m)$.

$$m \rightarrow \boxed{\text{fonction de chiffrement + clef}} \rightarrow E_k(m)$$

La fonction de *déchiffrement*, notée $D_k(c)$, permet de retrouver le message original m à partir d'un message chiffré $c = E_k(m)$ connaissant la clef de déchiffrement k.

$$c \rightarrow \boxed{\text{fonction de déchiffrement + clef}} \rightarrow D_k(c)$$

Ces fonctions vérifient l'équation $D_k(E_k(m)) = m$, ce qui permet de retrouver le message original avec la fonction de déchiffrement et le message chiffré. En général, ces fonctions reposent sur un problème « difficile » à résoudre. Ainsi, sans connaître la clef de déchiffrement, il est difficile de déchiffrer un message, et ce, tant qu'il n'existera pas de moyen de résoudre le problème dit « difficile ». Il existe deux catégories de chiffrement : les chiffrements symétriques et les chiffrements asymétriques, également appelés chiffrements à clef publique. Ces derniers chiffrements utilisent une paire de clefs comportant une clef publique et une clef privée (secrète). La figure 4 représente la notation utilisée dans cet ouvrage pour des clefs publiques, privées ou symétriques.

FIGURE 4 – Clef publique/clef privée asymétriques et clef symétrique.

Pour plus de détails, le livre référence de B. Schneier [Sch01a] et de nombreux autres ouvrages [Kob00, Buc01, DK02, DRTV13] présentent les différentes méthodes de chiffrement existantes. Parmi les chiffrements à clef publique il existe des chiffrements déterministes ou des chiffrements probabilistes : un chiffrement déterministe d'un message donne toujours le même chiffré, alors qu'un chiffrement probabiliste donne un chiffré différent à chaque chiffrement du même message.

Chiffrements symétriques

Les chiffrements symétriques utilisent la même clef pour chiffrer et déchiffrer un message. La protection de cette clef est cruciale pour la confidentialité des informations échangées. Les algorithmes de chiffrement symétrique reposent souvent sur des techniques de substitutions et de transpositions. Cela offre un moyen rapide et efficace pour chiffrer un message.

Le chiffrement « parfait » (chiffrement de Vernam)

Le chiffrement symétrique parfait (incassable au sens de la théorie de l'information) est le *chiffrement à masque jetable* (One-Time Pad) aussi appelé chiffrement de Vernam, car supposé avoir été découvert par le Major J. Mauborgne et G. Vernam en 1917, or d'après de récents travaux [Bel11] il fut inventé 35 ans plutôt par Frank Miller. Un masque jetable est une suite de bits aléatoires aussi longue que le message à chiffrer. Cette suite est un secret connu uniquement des deux participants et ne peut être utilisée qu'une seule fois. Le message original est codé sous forme de bits. Pour le chiffrer, chaque bit du masque est comparé au message. S'ils sont égaux, 0 est placé dans le message chiffré sinon 1 ; ceci revient à effectuer une addition bit à bit modulo 2. Connaissant le masque, il est alors facile de reconstituer le message original.
Malheureusement, ce chiffrement présente quelques inconvénients lors de sa mise en pratique car le masque doit être :
– aussi long que le message à chiffrer ;
– utilisé une seule fois ;
– généré de manière aléatoire pour éviter qu'il ne soit deviné ;
– échangé de manière sûre entre les participants.
Sans connaître le masque, il est prouvé sous ces conditions qu'il est impossible de retrouver le message original. Cependant, bien qu'inviolable en théorie, ces inconvénients le rendent finalement très complexe à utiliser en pratique.
Comme l'a bien souligné Steve Bellovin ⋆ :

> « As a practical person, I've observed that one-time pads are theoretically unbreakable, but practically very weak. By contrast, conventional ciphers are theoretically breakable, but practically strong. »

Il faut donc se tourner vers d'autres méthodes de chiffrement théoriquement vulnérables mais plus robustes en pratique.

« *Data Encryption Standard* » (DES)

Le 23 novembre 1976, le « *National Institute of Standards and Technology* » (NIST) adopte le standard de chiffrement DES [NBS80, NBS77, NBS88]. Ce chiffrement conçu par IBM sous le nom de LUCIFER a été choisi par le NIST après quelques modifications. Ce chiffrement symétrique permet de chiffrer des messages de 64 bits avec une clef k de 56 bits. Le chiffrement DES est constitué de 16 enchaînements successifs de

⋆. En tant que personne pratique, j'ai observé que les chiffrements à masque jetable sont théoriquement incassables, mais en pratique très faibles. Au contraire, les chiffrements classiques sont théoriquement cassables, mais en pratique sûrs.

la fonction de Feistel, qui effectue successivement des opérations de transposition, de substitution et de chiffrement de Vernam.
Les avancées matérielles en informatique permettent aujourd'hui, en un temps raisonnable de « casser » un message chiffré avec DES par *force brute*, ce qui consiste à tester toutes les clefs possibles grâce à une énumération exhaustive. En 1998, le NIST lança un appel d'offres pour choisir le nouveau standard de chiffrement symétrique, l'« *Advanced Encryption Standard* » (AES) qui est le successeur du DES devenu trop sensible aux attaques par recherches exhaustives.

« *Advanced Encryption Standard* » (AES)

Le standard de chiffrement symétrique AES fut donc adopté en 2000 par le NIST en remplacement du DES. Son nom original est *Rijndael* et il a été conçu par V. Rijmen et J. Daemen [DR02]. Ce chiffrement est constitué de substitutions, de décalages, de « ou exclusif » et de multiplications par un polynôme fixé, dans un anneau fini ; ces opérations sont élémentaires, simples et rapides à calculer. Il permet de chiffrer des blocs de 128 bits en utilisant des clefs symétriques de 128, 192 ou 256 bits. Il y a donc au total trois combinaisons possibles. Ceci laisse une plus grande flexibilité à l'utilisateur d'AES en fonction du niveau de sécurité et de la vitesse de calcul désirés.

Modes de chiffrement symétrique

Pour chiffrer un texte plus long que les messages acceptés par un chiffrement symétrique, une méthode naïve consiste à découper en blocs (souvent de 64 ou 128 bits) le message puis à appliquer le chiffrement sur chacun des blocs. Ce procédé est le *mode de chiffrement par blocs* appelé « *Electronic Code Book* » (ECB). Il n'est pas le plus sécurisé des modes de chiffrement. D'autres modes comme « *Cipher Block Chaining* » (CBC), « *CounTeR mode encryption* » (CTR) ou « *Galois Counter Mode* » (GCM) sont aujourd'hui préconisés par le NIST.

Chiffrements asymétriques

Un chiffrement asymétrique utilise une clef de chiffrement différente de celle de déchiffrement. La clef de chiffrement est souvent connue de tous les agents, elle est appelée *clef publique* et permet de construire un message chiffré. Cependant seuls les participants connaissant la clef de déchiffrement, appelée *clef privée*, peuvent déchiffrer les messages. Les chiffrements asymétriques reposent sur l'existence de fonctions mathématiques dites à *sens unique* ou à *sens unique avec trappe*. Une fonction à sens unique est une fonction mathématique facilement calculable mais dont la réciproque est, en pratique, impossible à calculer car trop coûteuse en temps ou en ressources. Par exemple, le produit de deux grands nombres premiers est une opération mathématique simple, mais trouver à partir de ce produit les deux nombres premiers est un problème connu difficile. Ce problème est appelé *problème de la factorisation*.
Les fonctions à sens unique avec trappe sont, elles aussi, facilement calculables mais leur réciproque est difficile à effectuer sans connaître l'information secrète : la trappe. Ainsi, la factorisation en produit de deux nombres premiers est une fonction à sens

unique avec trappe : connaissant un des deux nombres premiers, il devient alors aisé par une simple division de retrouver le second nombre premier.
Le chiffrement Rivest-Shamir-Adleman (RSA) [RSA78], l'un des plus utilisés, a été inventé en 1978, et repose sur le problème difficile de la factorisation d'un entier en produit de deux grands nombres premiers. Il existe de nombreuses méthodes de chiffrements asymétriques. Elles sont souvent rattachées à un problème mathématique difficile, comme le chiffrement de Rabin, inventé en 1979, reposant, lui, sur le problème difficile des racines carrées dans un corps fini ou le chiffrement d'Elgamal inventé en 1985 qui s'appuie sur la difficulté de résoudre le problème du logarithme discret [Elg85].

Avantages et inconvénients des chiffrements symétriques et asymétriques

Les opérations de calculs pour un chiffrement symétrique sont plus rapides et utilisent des clefs de tailles plus petites qu'un chiffrement asymétrique pour un même niveau de sécurité. Un chiffrement symétrique utilise des fonctions mathématiques simples et par conséquent facilement implémentables au niveau matériel, dans des composants électroniques. Par contre, un cloisonnement fort des échanges nécessite une clef différente par couple de participants. Le chiffrement symétrique impose alors la distribution d'un grand nombre de clefs, sachant que la divulgation de la clef rendrait caduque la sécurité appliquée à la communication.
Un chiffrement asymétrique permet quant à lui d'authentifier l'expéditeur d'un message car la clef privée est unique et propre à un participant donné. Cette preuve d'origine en chiffrement symétrique n'est pas possible, la clef étant connue d'au moins deux participants. Par ailleurs, la distribution des clefs publiques est très simple à gérer avec ce genre de chiffrement. Cependant, cette méthode utilise des clefs de grandes tailles et nécessite un temps de calcul plus long et plus de ressources que lors d'un chiffrement symétrique, ceci à cause de la complexité des opérations à effectuer.
Dans les deux cas, l'authenticité des clefs cryptographiques est essentielle, c'est-à-dire la preuve que la clef cryptographique fournie est bien celle qui devait être reçue et provient d'une source de confiance.
En pratique, chiffrements symétrique et asymétrique sont utilisés conjointement dans les applications et la sécurisation des échanges, afin d'allier leurs avantages. Généralement, le chiffrement symétrique est utilisé pour :
- le chiffrement de communications (données et voix) et de messages de grandes tailles ;
- la protection en intégrité de ces mêmes communications et messages ;
- la preuve de connaissance d'un secret.

Alors que le chiffrement asymétrique s'utilise pour :
- le chiffrement de messages de petites tailles pour des destinataires précis, tel l'envoi d'une clef symétrique par exemple ;
- la preuve d'origine de données (ainsi nommée signature), d'un message, d'un document, d'un tampon d'horodatage, d'un logiciel ;
- la non-répudiation d'un contrat.

Autres primitives cryptographiques

Il existe de nombreuses autres primitives cryptographiques permettant de réaliser d'autres fonctionnalités. La cryptographie à clef publique permet par exemple de réaliser facilement des *signatures*. Pour signer un message, il suffit de le chiffrer avec la clef privée. Toute personne connaissant la clef publique, le message original et le message signé peut utiliser la clef publique sur le message signé pour retrouver le message original. Le seul moyen d'avoir pu générer une signature valide est de posséder la clef privée, ainsi la personne en possession du message signé est sûre que ce message a été produit par la personne possédant la clef privée. La preuve d'origine est alors garantie.
Une autre primitive cryptographique est la *fonction de hachage* qui est une fonction déterministe prenant en entrée un message de n'importe quelle taille, noté $\{0,1\}^*$, et calcule une empreinte de taille fixe (en général 128 ou 256 bits). Ces fonctions sont difficiles à inverser et il est difficile de trouver deux messages ayant la même empreinte. Ces fonctions sont par ailleurs très rapides d'exécution et permettent de garantir l'intégrité du message original. En possédant un message et son empreinte et en recalculant l'empreinte du message avec la fonction de hachage, il est possible de détecter si le message orignal a été modifié par comparaison des empreintes.
Il existe des fonctions de hachage qui, en plus d'un message, prennent en entrée une clef secrète, ces fonctions sont appelées codes d'authentification de message (« *Message Authentication Code* », MAC). Elles offrent la garantie que l'empreinte ne peut être correctement calculée qu'en possession de la clef secrète. Elles seront présentées en détail au chapitre 2 et utilisées dans de nombreux protocoles dans la suite du livre.

Architecture à clef publique

Un des principaux défis en sécurité réside dans l'échange de clefs symétriques afin de garantir une communication efficace et sécurisée entre deux entités. Comme évoqué précédemment, cet échange doit être réalisé de manière à garantir :
– la confidentialité des clefs secrètes ;
– l'intégrité de ces clefs ;
– leur authenticité.
En 1976, Diffie et Hellman proposent un premier protocole d'échange de clefs utilisant la commutativité des puissances en arithmétique modulaire. Ce protocole permet d'établir une nouvelle clef secrète partagée entre deux entités, mais il ne garantit pas l'authentification des participants, c'est-à-dire qu'il est possible que la clef échangée le soit avec un autre participant que celui escompté. Le premier algorithme de chiffrement à clef publique RSA (1978) constitue une avancée considérable pour résoudre ce problème. Après plusieurs tentatives de solutions, il est désormais possible d'échanger une clef de manière sûre et authentifiée entre deux personnes. L'ensemble des mécanismes permettant cet échange sécurisé est appelé architecture à clef publique ou encore Infrastructure de Gestion de Clefs (IGC), soit PKI en anglais, et constitue l'objet de cet ouvrage.

Chapitre 1

Motivations pour une architecture asymétrique

Pour gérer des clefs asymétriques, il est nécessaire d'utiliser une Infrastructure de Gestion de Clefs (IGC) (« *Public Key Infrastructure* », PKI), formée d'un ensemble d'éléments permettant de réaliser effectivement des échanges sécurisés. En effet, une fois des algorithmes cryptographiques asymétriques complexes définis, le premier problème pratique qui se pose est celui de l'affiliation d'une clef publique à son propriétaire. Le principe des PKI repose sur la diffusion de métadonnées en plus de la clef publique. Ces métadonnées contiennent des données d'identification du propriétaire de la clef et permettent de les lier sans ambiguïté à une clef publique. Parmi ces données peuvent se trouver l'état civil, l'adresse postale, l'adresse de messagerie électronique, un nom de domaine ou encore l'adresse IP d'un serveur. Le terme certificat numérique est employé pour désigner le conteneur regroupant ces métadonnées, la clef publique et la signature numérique qui lie et authentifie l'ensemble. La création et la gestion de ces certificats sont assurées par la PKI. Plus de détails sur ce sujet sont abordés dans le chapitre 3.

Le présent chapitre se concentre sur les conditions dans lesquelles une architecture asymétrique est nécessaire. Tout d'abord, la solution théorique parfaite pour échanger des clefs est donnée dans le paragraphe 1.1 : il s'agit du protocole de Diffie-Hellman qui permet qu'un secret complet ne transite jamais sur un canal. Les étapes du protocole sont symétriques pour les participants, mais il nécessite une mise en commun préalable, éventuellement même en clair, de paramètres. Néanmoins, en pratique, ce protocole est soumis à des attaques de type « *Man-In-The-Middle* » où un attaquant actif peut se faire passer tour à tour pour chacun des participants du protocole. L'attaquant peut ainsi en toute impunité se faire passer pour un participant auprès d'un autre.

Une solution pour contrecarrer cette attaque est l'utilisation d'un *tiers de confiance*, qui connaît préalablement les acteurs désirant communiquer, et va se charger de leur authentification. Il existe un protocole à tiers de confiance n'utilisant que de la cryptographie symétrique, *Kerberos*, décrit dans le paragraphe 1.2.

Toutefois, ce système a un inconvénient principal, inhérent à l'utilisation de clefs symétriques : le tiers de confiance doit être infaillible, puisqu'il connaît les clefs de la totalité des utilisateurs du système. En particulier, il est capable d'écouter toutes les conversations, et s'il est attaqué avec succès, toutes les clefs doivent être changées. Pour pallier ce problème, une solution est de préférer un système à clef publique pour l'authentification. En effet, dans les architectures à clefs publiques, le tiers de confiance ne peut pas accéder aux communications des participants et, s'il est compromis, seule sa capacité d'authentification est altérée. Le principal général de fonctionnement des architectures à clefs publiques est donné dans le paragraphe 1.3. Les détails techniques et structurels sont présentés aux chapitres suivants.

1.1 Authentification et partage de clefs

Afin de pouvoir échanger une information confidentielle, la cryptographie symétrique a besoin de secrets partagés. Ce secret commun peut être directement la clef secrète symétrique ou des données permettant de reconstruire une telle clef. La question est de savoir comment partager un secret. Pour une sécurité parfaite par exemple, deux acteurs devraient se rencontrer en personne et trouver un moyen d'échanger ce secret de manière protégée. Cela peut ne pas être très pratique. Une alternative est d'utiliser des outils cryptographiques pour effectuer cet échange de clefs. Le protocole de Diffie-Hellman inventé en 1976 permet d'éviter cette rencontre physique en faisant en sorte que le secret complet ne transite jamais sur aucun canal.

1.1.1 Protocole d'échange de clef secrète de Diffie-Hellman

L'utilisation d'une fonction à sens unique comme l'exponentiation modulaire est au cœur du protocole de Diffie-Hellman et permet le partage de clefs. Supposons donc qu'Alice et Bob souhaitent partager une clef secrète K. Ils conviennent d'abord d'un entier premier p et d'un générateur g de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$.
En deux échanges de message, Alice et Bob construisent une clef partagée secrète K :

1. (a) Alice choisit un nombre $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ secret et calcule $A := g^a \mod p$. Elle envoie A à Bob.
   (b) Symétriquement, Bob choisit un nombre $b \in \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ secret et calcule $B := g^b \mod p$. Il envoie B à Alice.
2. (a) Alice calcule alors $B^a \mod p$.
   (b) Symétriquement, Bob calcule de son côté $A^b \mod p$.

À la fin, Alice et Bob partagent la même clef secrète $K = g^{a.b} \mod p$ sans l'avoir jamais communiquée directement. Le protocole d'échange de clef de Diffie-Hellman est décrit dans la figure 1.1.

Exercice 1.1. *Exemple de clef Diffie-Hellman.*
Alice et Bob conviennent des paramètres suivants : $p := 541$ et $g := 2$. Alice génère le nombre secret $a := 292$. De son coté, Bob génère le nombre $b := 426$. Quelle est la clef secrète résultant du protocole d'échange de Diffie-Hellman ?

Solution de l'exercice en page 319.

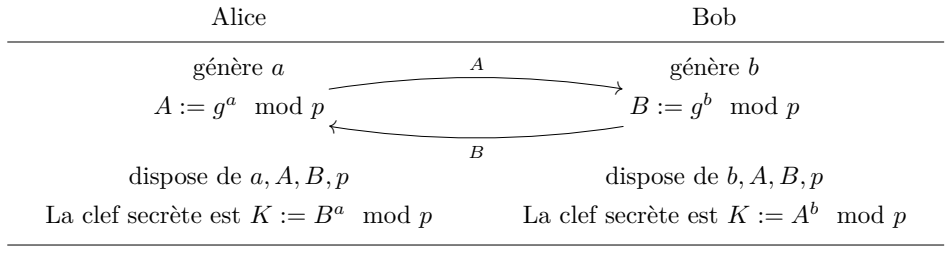

FIGURE 1.1 – Protocole de Diffie-Hellman (1976).

Exercice 1.2. *Sécurité de Diffie-Hellman.*
Oscar voit passer A et B, expliquer pourquoi Oscar ne peut alors pas facilement en déduire K.

Solution de l'exercice en page 319.

1.1.2 Attaque « *Man-in-the-middle* »

L'inconvénient majeur du protocole de Diffie-Hellman est qu'il est sensible à une attaque dite « *Man-In-The-Middle* » (MITM). Cette faiblesse repose sur le fait qu'un adversaire actif (Oscar) placé entre Alice et Bob peut intercepter toutes les communications, et ainsi se faire passer pour Bob auprès d'Alice et simultanément pour Alice auprès de Bob. Oscar peut alors lire toutes les communications entre Alice et Bob avec la clef qu'ils pensent avoir construite en secret.
En pratique Oscar fabrique a' et b'. Il intercepte ensuite A et B puis fabrique $K_A := A^{b'}$ et $K_B := B^{a'}$. Il envoie ensuite $g^{b'}$ à Alice et $g^{a'}$ à Bob. L'évolution de l'attaque est illustrée dans la table 1.1.

Alice	Oscar	Bob
génère a	génère b' et a'	génère b
$A := g^a \mod p$	A → $A' := g^{a'} \mod p$	A' → $B := g^b \mod p$
	B' ← $B' := g^{b'} \mod p$	B ←
connaît a, A, B'	a', A, B', b', B, A'	connaît b, A', B
Clef secrète :	Clefs secrètes :	Clef secrète :
$K_A := B'^a \mod p$	K_A et K_B	$K_B := A'^b \mod p$

TABLE 1.1 – Attaque MITM dans le protocole d'échange de clef de Diffie-Hellman.

Ensuite, Oscar doit déchiffrer à la volée les messages envoyés par Alice ou Bob, puis les chiffrer avec l'autre clef de la manière décrite dans la table 1.2.

Alice	Oscar	Bob
$C := E_{K_A}(M)$	$\xrightarrow{C}$	
	$M := D_{K_A}(C)$	
	$\Gamma := E_{K_B}(M)$	$\xrightarrow{\Gamma}$
		$M := D_{K_B}(C)$

TABLE 1.2 – Envoi de message intercepté par le MITM.

Finalement, Alice et Bob croient s'envoyer des messages secrets, alors qu'Oscar les intercepte et les déchiffre. Oscar est donc non seulement capable d'obtenir en clair tous les échanges entre Alice et Bob, mais en outre il peut modifier ces échanges. En effet, rien ne l'empêche, au cours de l'interception, de remplacer le message envoyé par Alice par une autre information.

Exercice 1.3. *Échange de clefs authentifié.*
Soit un protocole à clef publique inspiré de l'échange de clef de Diffie-Hellman, dans lequel les entités s'authentifieraient.
Les paramètres publics sont les suivants :
– un grand nombre premier p ;
– un grand facteur premier q de $p-1$;
– un élément g d'ordre q dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$..
Chaque utilisateur U possède un secret aléatoire $X_U \in \left(\mathbb{Z}/q\mathbb{Z}\right)^*$, et une clef publique $Y_U = g^{X_U} \mod p$. Toutes les clefs publiques des utilisateurs sont stockées dans une base de données authentifiée (*e.g.,* grâce à un tiers de confiance), qui est accessible publiquement. Soit le protocole de mise en commun de clef suivant :
– A génère $a \in \left(\mathbb{Z}/q\mathbb{Z}\right)^*$ avec un « *PseudoRandom Number Generator* » (PRNG), calcule $v := g^a \mod p$, et envoie v à B.
– B génère $b \in \left(\mathbb{Z}/q\mathbb{Z}\right)^*$ avec un PRNG, calcule $w := g^b \mod p$ et envoie w à A.
Au final, A et B partagent la clef secrète $K = g^{aX_B + bX_A} \mod p$.

1. Expliquer comment A peut effectivement calculer K.
2. En supposant que le PRNG est biaisé dans le sens qu'il ne génère que des petits nombres (*e.g.,* de taille autour de 40 bits) au lieu de générer des nombres presque uniformément dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^*$. Montrer comment un adversaire E peut apprendre K. Proposer une contre-mesure.
3. En supposant que $b = ac$ pour un petit c, montrer qu'un adversaire E peut également déduire K. Proposer une contre-mesure.

Solution de l'exercice en page 319.