Eléments rapides de cryptologie

Eric DUPUIS[1,2]*

Résumé
Ce document fournit quelques éléments de synthèse dans le domaine de la cryptologie
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel au cours.

Mots clefs
Cryptologie, synthèse

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@lecnam.net – eric.dupuis@orange.com

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C2-Crypto.pdf

A une époque où chaque jour la presse se fait régulièrement écho de pertes ou de vols de données, où l'Europe déploie son corpus réglementaire autour de la protection des données personnelles, certains s'interrogent encore sur les moyens de protéger et partager de manière sûre son patrimoine informationnel. La cryptographie est une des disciplines de la cryptologie qui s'attache à protéger ces patrimoines en confidentialité, intégrité ou en authenticité. Au-delà des aspects mathématiques passionnants, quels sont les usages et les arcanes techniques de ces technologies ?

1. Définitions

La cryptologie est par étymologie la science du secret. Elle regroupe la cryptographie, qui porte sur les moyens de coder et décoder les messages, et la cryptanalyse, qui permet de les déchiffrer (de manière non coopérative !). Ces techniques remontent à la nuit des temps. Historiquement militaires et diplomatiques, elles sont devenues civiles avec l'avènement de technologies de l'information, dont la carte à puce [2] et l'internet.

Elles ont envahi à grande vitesse toutes les technologies numériques.« Signer, protéger, imputer, authentifier... » sont devenus des termes courants de cette vie numérique. On est toutefois surpris de l'usage, quelquefois un peu« dévoyé », de certaines expressions.« Crypter » s'oppose à« décrypter », mais si décrypter, c'est« décoder » sans connaître les secrets, crypter est humoristiquement enterrer mettre en« crypte »! Si les expressions« coder » et« décoder » sont régulièrement utilisées, celles préconisées sont« chiffrer » et« déchiffrer ». En France, au sein des armées, les acteurs du domaine se nomment d'ailleurs des spécialistes du chiffre [3]. Face à un spécialiste, du mathématicien cryptologue au commercial de services numériques de confiance, de nombreux termes se bousculent dans les discussions : algorithmes robustes de niveau militaire, clefs très longues, protocoles sûrs, certificats de confiance...

2. Des concepts

Derrière ces arguments qui pourraient, au premier abord, paraître convaincants, il convient rapidement d'opposer une petite analyse terminologique et conceptuelle.

2.1 Algorithmes

Le nombre d'algorithmes mathématiques (fonctions mathématiques) en cryptographie est presque aussi grand que le nombre de mathématiciens qui travaillent dans le domaine. Il faut y ajouter le nombre d'implémentations informatiques de chaque algorithme, sans compter les différents langages utilisés pour la même implémentation. Quelques grandes révolutions ont eu lieu depuis le chiffre de César, mécanisme de chiffrement par décalage« alphabétique » utilisé dans notre enfance, et celui de la machine allemande Enigma de la dernière guerre, avec des mécanismes de substitution dits polyalphabétiques. Ces évolutions et révolutions ont lieu chaque fois que ces fameux cryptanalystes trouvent ou

2. téléphonie mobile (SIM) et carte bancaire.
3. ARCSI : Association des réservistes du chiffre et de la sécurité de l'information - www.arcsi.fr

entrevoient une solution pour casser ce chiffre... Une longue tradition dans cette course entre la cuirasse et le canon.

2.1.1 Le chiffrement à clefs secrètes

Ces premiers algorithmes dits symétriques ou à clefs secrètes ont été et restent centraux, car ils se révèlent très rapides. Le principe est que pour déchiffrer, il faut simplement la clef qui a servi à chiffrer, d'où le terme« symétrique ». Une des grandes difficultés dans ces algorithmes est la combinatoire pour partager le secret. Si partager de manière sûre un secret entre deux ou trois correspondants est maîtrisable, le faire pour mille ne permet plus vraiment de parler d'une clef secrète ! L'histoire des célébrités technologiques retient des algorithmes comme DES, 3DES, IDEA, RC4 et le dernier réputé inviolé et issu d'un appel à projet du NIST[4] et paru dans les années 2000 : AES256.

2.1.2 Cryptographie à clefs publiques

Le chiffrement asymétrique résout ce problème de la combinatoire, mais reste bien plus lent. Rendu célèbre par Alice et Bob, deux personnages illustrant les cours de cryptologie asymétrique, ce mécanisme utilise une paire de clés liées dites asymétriques : une clé publique et une clé privée. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète. Pour cette une paire de clés, les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante (donc si vous avez la clef publique de votre correspondant, vous pouvez chiffrer une information pour lui). Inversement, les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'avec la clé publique correspondante. Cette caractéristique est utilisée pour mettre en œuvre la signature numérique.

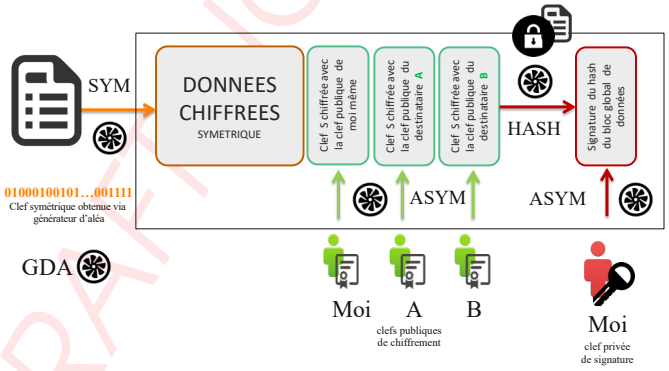

FIGURE 1. Exemple d'une encapsulation asymétrique pour un chiffrement de fichier

2.2 Fonction de hashage

Les fonctions de hachage cryptographique (de l'anglais« hash ») sont présentes dans tous nos systèmes numériques. Ce sont des fonctions rapides à sens unique qui permettent de transformer tout bloc d'information de taille quelconque et une donnée de taille fixe

4. National institute of standards and technology.

souvent courte. Ce mécanisme, qui permet de prendre une« empreinte » des données, est à la base des mécanismes de signature, de contrôle d'intégrité et de stockage de mots de passe. Les algorithmes les plus connus sont md5, sha1 et maintenant sha256, sha512 nécessaires par les fragilités découvertes sur les premiers, car ces algorithmes sont aussi sujets aux attaques !

2.3 Clefs

Au cœur de la cryptographie, les clefs restent l'objet de toutes les attentions. Il est conseillé la lecture des quelques documents de référence de l'Anssi [5] sur les« mécanismes cryptographiques »[6] qui illustrent de manière pragmatique et concrète cette indispensable vigilance.

2.3.1 Taille de clefs

Un des débats dans l'usage de la cryptographie concerne la taille optimale des clefs. Ce sujet fait l'objet de nombreuses publications. Pour les algorithmes symétriques, 1 280 bits est la taille de référence (soient 2 puissance 128 possibilités). La notion de taille de clefs pour les algorithmes asymétriques est moins simple. Cela dépend des problèmes mathématiques sous-jacents. Pour le plus célèbre RSA [7] (6), qui aura bientôt 40 ans, les experts considèrent qu'une taille de 2 048 est à l'état de l'art jusqu'en 2030. RSA est utilisé pour les transactions pour la carte bleue, les achats sur internet, les courriels sécurisés. Pour ceux basés sur le logarithme discret, la taille préconisée est de 200 bits, pour les courbes elliptiques de 256 bits. Il est donc important de spécifier les algorithmes pour comparer des tailles de clefs.

2.3.2 Aléas et générateur d'aléas

De nos jours, une bonne clef secrète est très rarement issue de notre cerveau (même un bon mot passe mémorisable est totalement perfectible sur le pur plan cryptographique) [8]. Pour générer des clefs d'un bon niveau cryptographique, c'est-à-dire non sujettes à des biais de prédiction possibles, il est nécessaire d'utiliser un générateur de nombres aléatoires (GDA ou RNG : « random number generator ») de qualité cryptographique. Il est fondamentalement complexe de générer de véritables nombres aléatoires. Le processus de génération d'aléas doit comporter des sources fondamentalement aléatoires (bruit électronique, thermique dans des composants) combinées à des sources multiples (hash d'une zone mémoire...), le tout passé à la moulinette d'algorithmes de pseudo-aléas suffisamment imprévisibles. Ce fondamental de la cryptologie est un domaine de recherche à part entière. C'est aussi une activité industrielle autour des HSM (hardware security module) pour la génération rapide, le stockage et la protection des clefs primordiales pour les transactions numériques bancaires en particulier.

5. Anssi : Agence nationale pour la sécurité des sytème d'information, services du Premier ministre.
6. Annexe B1 et B2 du RGS V2 (Anssi : référentiel général de sécurité) : Mécanismes cryptographiques et gestion des clefs.
7. 1978, apparition de l'algorithme à clef publique de Rivest, Shamir et Adelman (RSA).
8. Un mot de passe de qualité« cryptographique » devrait être d'au moins 20 caractères dans un alphabet de 90 symboles.

2.3.3 Protocoles et formats

De bons algorithmes, de bonnes clefs ne suffisent pas. Il est indispensable de s'assurer de l'ensemble des mécanismes qui vont permettre de garantir que« les secrets échangés » restent bien secrets. On parle de protocole d'authentification, de signature, d'échange de clefs (Kerberos, Diffie Elmann, RSA...). C'est souvent au cœur de ces protocoles qui nécessitent une attention particulière en termes de robustesse et de preuve formelle que l'on trouve des vulnérabilités. Le format des données chiffrées (cf Fig. 2) est aussi une source de fragilité (cacher une partie de la clef en piégeant l'ordinateur, exploiter une vulnérabilité logicielle). Les solutions technologiques de chiffrement combinent pour des raisons de performance des mécanismes de chiffrement symétrique et asymétrique.

2.3.4 Certificats

Le terme« certificat électronique » est entré dans le langage courant du numérique :« Certificat machine, serveur »,« certificat utilisateur ». à la base des usages des systèmes à clefs publiques, ce certificat contient la (les) clef(s) publique(s), des informations d'identification, des dates de validité, et un mécanisme de signature garantissant l'origine. Informatiquement ce« paquet » de données nécessite des standards de formats structurés interopérables comme le codage X.509 ou le stockage PKCS12.

2.3.5 Certificats auto-signés !

Une clef publique« valide » dans un système cryptographique de confiance, doit être signée par une autorité de confiance pour être vérifiée par la suite par son« usager ». Disposer d'une PKI ou faire certifier sa chaîne de confiance est complexe et coûteux. Le monde informatique fait donc largement usage de l'auto-signature, c'est-à-dire de la génération des clefs, sans chaîne de confiance partagée. Lorsque les logiciels sont permissifs sur ces usages, l'ensemble du système est fragilisé.

2.3.6 IGC ou PKI

Utiliser des mécanismes à clefs publiques nécessite donc l'utilisation d'un ensemble interopérable de confiance (algorithmes, protocoles, formats) permettant de générer les clefs (couple privée/publique), de les attribuer, de les signer (les certifier), de les distribuer, et de les révoquer (les supprimer de l'environnement de confiance). L'ensemble de ces mécanismes s'appelle une IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure). Ces outils logiciels et l'organisation globale sont indispensables à un usage structuré de confiance. Sans cette maîtrise des clefs, un système à clef publique peut s'effondrer. En effet, si des clefs de certification, ou des clefs privées d'utilisateurs sont compromises à la source, la résistance mathématique des algorithmes ou des protocoles ne vous garantira plus grand-chose... C'est dans cet esprit que sont nés les tiers de confiance, qui vous assurent que toutes les précautions sont prises pour protéger cette chaîne.

3. De la confiance aux usages en entreprise

Comme vous l'avez noté, un système cryptographique est un ensemble de briques (fig. 1) qu'il est nécessaire de contrôler pour définir un niveau de confiance de la chaîne. Si disposer d'outils à clefs publiques sans un IGC (PKI) se révèle fragile, disposer d'une IGC sans disposer d'une maîtrise des usages l'est autant... En France, le terme de moyen (9) cryptologique est défini par loi sur la confiance numérique, mais il est à remarquer que, dans l'entreprise, il se conjugue différemment en fonction des interlocuteurs :

- pour les équipes réseaux : la cryptologie est enfouie dans les méandres des protocoles des technologies des canaux sécurisés VPN, IPSEC, VPN, chiffreurs réseaux ;
- pour les équipes des services informatiques : le déploiement, la mise à jour des certificats sur des terminaux et des serveurs concentrent une bonne partie des problèmes opérationnels ;
- pour la bureautique et le poste de travail : les produits et les services pour chiffrer les données et préserver la confidentialité dans les messageries ou sur les supports (smartdevice, disques, USB, serveur de fichiers) sont complexes à choisir pour l'interopérabilité ;
- pour les métiers de l'entreprise comme les achats ou l'archivage probant, les enjeux d'authenticité, d'imputabilité et d'intégrité ainsi que la signature électronique nécessitent des travaux transverses à l'entreprise souvent coûteux.

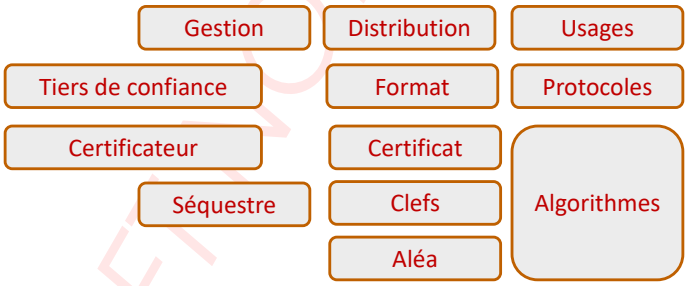

FIGURE 2. Les briques à vérifier dans la chaine de confiance

Il est à noter, le point particulier du recouvrement des données chiffrées et du séquestre des clefs. Indispensable pour les malchanceux qui perdent leur clef privée ou par nécessité (départ de l'entreprise, réquisition sur des données...), la confiance dans celui qui possède cette capacité de recouvrement est un enjeu fondamental. Acquérir et déployer un système cryptographique dans l'entreprise doit se baser sur un minimum de confiance dans l'implémentation des briques. Il est important que ces produits aient été analysés, vérifiés par des tiers (entre le constructeur ou éditeur et l'utilisateur ou acheteur). On parle ainsi de certifications de produits au titre de la norme de l'Iso 15408 (critères communs), qualification de produits et de services par l'Anssi. Perturbant un peu l'écosystème et les frontières de gouvernance des DSI, l'usage des services dans le cloud nécessite

de nouvelles technologies de chiffrement pour maintenir la confidentialité totale, mais autoriser quand même des traitements. Le chiffre homomorphe permet justement à un système tiers d'opérer des calculs sur des données chiffrées sans les déchiffrer et ainsi récupérer les résultats exploitables. Des solutions matures arrivent sur le marché depuis peu.

3.1 De l'usure électronique au partage de confiance

3.1.1 Usure ou rupture cryptographique

Si le temps n'est pas l'ami de l'archivage, il ne l'est pas non plus du chiffrement. Non par l'usure du support, mais simplement par la complexité d'une longue conservation des clefs, de l'érosion de la résistance des mécanismes. En outre, depuis des années, le terme« quantique » est apparu dans la littérature du domaine. Si la distribution quantique offre une transmission sûre de clef, l'ordinateur quantique pourrait apporter cette rupture que redoute l'industrie numérique, car capable de rompre la solidité des problèmes mathématiques sur lesquels repose une grande partie des mécanismes cryptographiques actuels.

3.1.2 Bitcoin, blockchain...

Nous avons rapidement parcouru l'usage courant de la cryptographie en entreprise, mais de nouvelles révolutions des usages de la cryptographie sont déjà à nos portes. Après quelques années d'hésitation, la montée des« crypto-monnaie » comme Bitcoin donne une large expression aux mécanismes de signature pour assurer intégrité, traçabilité, imputabilité et modifie le rapport à la confiance« centralisée ». Dans l'émergence rapide de cette« décentralisation de la confiance », quelques positions établies sont remises en cause. On notera en particulier une forme naissante d'ubérisation des chaînes de confiance, qui bouscule déjà le marché effervescent de la sécurité.

Table des matières

Table des figures