Chapitre 2. Concepts de cryptographie et de cryptanalyse

Dr. Bouchene
Mohammed Mehdi

2019-2020

Sécurité de l'information

I. Exemples de la cryptographie dans le monde physique

Dans cette introduction, nous allons examiner pourquoi nous avons besoin de la cryptographie en premier lieu, et la meilleure façon de le faire est de regarder le monde physique. Un monde sans ordinateur, sans e-mail, sans iPad. Imaginez comment l'information existe dans ce monde et quelle est la sécurité de cette information. Ainsi, à la fin de cette section, vous devriez être en mesure d'identifier une gamme de mécanismes de sécurité utilisés dans le monde physique et appréciez pourquoi nous avons besoin de mécanismes de sécurité cryptographiques dans le monde numérique.

Nous pensons à cela par exmple la parole parlée dans la parole parlée, nous pouvons atteindre le secret en chuchotant et nous utilisons la proximité physique de deux personnes pour restreindre une conversation entre elles. De même, si nous avons dans une réunion dans une salle physique, nous fermons la porte, toutes les personnes présentes dans cette salle peuvent entendre les conversations qui ont lieu, les gens à l'extérieur de la salle ne peuvent pas. Nous utilisons donc souvent la présence physique pour guider le secret. Si des informations sont notées, nous disposons d'une gamme de techniques que nous utilisons. Nous mettons des lettres dans des enveloppes, nous pourrions mettre des morceaux de papier dans un classeur. Nous pourrions même verrouiller ce cabinet. Encore une fois, nous utilisons les mécanismes physiques du monde physique pour protéger les informations écrites. Un autre mécanisme de sécurité que nous voulons dans le monde physique est de s'assurer que les informations n'ont pas changé en aucune façon, soit délibéré, soit accidentel depuis sa création. Nous avons une multitude de techniques différentes que nous utilisons dans le monde physique pour ce faire. Peut-être que l'un des plus évidents est de coller une lettre dans une enveloppe et de la sceller, placer la lettre dans l'enveloppe est évidemment pour des raisons de secret. Mais si vous y réfléchissez, le sceau réel sur l'enveloppe est essentiellement une propriété qui nous permet de détecter si quelqu'un a ouvert cela ou peut-être changé le contenu. Autrefois, ils utilisaient également des cachets de cire pour une raison similaire. Il existe toutes sortes d'autres mécanismes que nous utilisons dans le monde physique.

Prenons par exemple un billet de 100 euros. Il s'agit d'informations écrites sur un objet physique et couvertes de mécanismes de protection, de mécanismes de protection physique, afin qu'elles ne puissent pas être falsifiées et ne puissent pas être modifiées. Vous pouvez choisir des marques d'eau, vous pouvez aussi choisir des hologrammes. Si vous regardez attentivement, il y a une bande sombre cette note, et c'est en soi un même la façon dont la note se sent est conçue pour détecter les changements pour détecter la contrefaçon. Un autre mécanisme de sécurité physique que nous utilisons est la signature manuscrite. Nous apposons notre signature sur des documents dans toutes sortes de situations. Fait intéressant, cela signifie de nombreuses propriétés de sécurité différentes. Mais une chose que nous considérons souvent

comme signifiant est la personne qui a signé ce document, atteste que les informations contenues dans ce document sont correctes et n'ont pas changé. Ce n'est peut-être pas le cas, mais nous utilisons beaucoup de signatures dans ce contexte.
Ces exemples montrent que dans le monde physique, il existe une gamme de mécanismes de sécurité physique, et que nous devons les remplacer dans le monde numérique.

II. Les principaux services et outils de sécurité de l'information fournis par la cryptographie

Dans cette section, nous allons considérer la cryptographie comme une boîte à outils, de mécanismes et d'outils, qui peuvent fournir différents types de sécurité dans le monde numérique et nous allons examiner certains de ces outils. À la fin de cette section, vous pourrez discuter de certains des principaux services de sécurité fournis à l'aide de la cryptographie et vous pourrez nommer plusieurs mécanismes cryptographiques qui fournissent ces services.

Confidentialité

Maintenant, il est important de reconnaître que la cryptographie ne fournira pas un remplacement individuel des mécanismes de sécurité dans le monde physique, mais qu'elle va essayer de remplacer les choses qui manquent dans ce monde numérique, et la première, et encore une fois, la propriété la plus évidente que nous voulons considérer au sujet de l'information dans le monde numérique, est le secret, la nécessité de s'assurer que seuls les destinataires désignés peuvent apprendre le contenu de l'information. Nous avons vu dans ce monde physique qui était souvent fourni par la proximité physique, ou par des boîtes et des serrures et des choses comme ça. Il s'agit donc du service de sécurité que nous appelons la **confidentialité**, la nécessité de s'assurer que les informations ne sont limitées qu'aux participants prévus.

Le mécanisme cryptographique que nous utilisons pour implémenter la confidentialité est le **chiffrement**. Nous avons une gamme d'outils pour fournir que :

- Le cryptage de chaîne,
- Chiffrement par bloc,
- Le cryptage à clé publique,

Ils relèvent tous de la rubrique chiffrement. C'est le premier outil.

Intégrité des données

Un service de sécurité très différent mais tout aussi important dont nous avons besoin dans le monde numérique que nous avons vue appeler **l'intégrité des données**. L'intégrité des données est vraiment une assurance que les données n'ont pas été altérées ou changées accidentellement ou délibérément avant que quelqu'un ne les lise où s'y fie. Maintenant, il existe une gamme d'outils cryptographiques pour fournir l'intégrité des données, et ceux-ci varient en fait dans la force d'intégrité qu'ils fournissent. Nous avons donc des outils tels que :

- Fonctions de hachage.
- Code d'authentification de message (MAC, Message Authentication Code)
- Signatures numériques

Qui sont tous utilisés pour assurer l'intégrité des données. Une fonction de hachage, par exemple, est un outil qui ne peut détecter que les modifications accidentelles des données. Si nous voulons une plus grande intégrité des données, nous avons besoin d'outils plus puissants.

Authentification de l'origine des données

Une propriété plus forte que l'intégrité des données est ce que nous appelons l'authentification de l'origine des données. Ainsi, l'authentification de l'origine des données garantit non seulement que les données n'ont pas été modifiées, mais fournit en fait une sorte d'assurance quant à la personne qui a envoyé les données. Ceci est parfois appelé authentification de message. Un mécanisme d'authentification de l'origine des données nous permettra donc de vérifier que les données n'ont pas été modifiées et nous donnera une assurance quant à leur provenance.

Non-répudiation

Un mécanisme encore plus puissant de celui-ci du service de sécurité est la non-répudiation. Ainsi, la non-répudiation nous donne en fait une garantie que non seulement les données n'ont pas été modifiées et que nous savons d'où elles proviennent, mais que celui qui nous a envoyé ces données ne peut pas nier plus tard qu'il nous a envoyé ces données. Maintenant, si vous y réfléchissez, une signature manuscrite dans un certain sens est un analogue de cela. C'est quelque chose que nous présentons au tribunal sur un contrat pour suggérer que les données doivent provenir de quelqu'un parce qu'il a signé le document. Mais si vous pensez à cette signature manuscrite, il est assez facile de modifier un contrat

après que quelqu'un l'a signé, et cela nous montre que ces outils cryptographiques que nous construisons peuvent en fait être plus forts que cela.

Le mécanisme cryptographique que nous utilisons pour la non-répudiation est la signature numérique. La signature numérique nous donnera également l'assurance que les données n'ont pas été modifiées de quel que soit la manière, car la signature sera différente sur un type de document différent.

L'intégrité des données, l'authentification de l'origine des données et la non-répudiation sont donc tous des outils importants qui nous aident à détecter si les informations ont changé.

Authentification des entités

Maintenant, il existe un autre service de sécurité que nous pourrions souvent souhaiter dans le monde numérique, un autre type d'authentification, et ce n'est pas l'authentification des données et des messages, c'est vraiment la réponse à la question simple qui est là-bas ? Donc, si vous considérez lorsque vous vous connectez à un appareil, un ordinateur, un iPad, l'appareil dit immédiatement qui est là-bas, qui utilise cet appareil, qui êtes-vous ? et nous avons une gamme de mécanismes de sécurité pour ce faire, y compris des choses comme les mots de passe, les codes d'accès, la biométrie, les empreintes digitales. Maintenant, ceux-ci ne sont pas intrinsèquement cryptographiques, bien que la cryptographie puisse être utilisée pour les implémenter. Mais la cryptographie fournit également des moyens très, très puissants de vous identifier.

En résumé, la cryptographie est une boîte à outils de différents mécanismes et nous avons parlé des principaux services de sécurité fournis par la cryptographie.

- Confidentialité,
- Intégrité des données,
- Authentification de l'origine des données,
- Non-répudiation
- Authentification des entités.

En fait, la cryptographie fournit beaucoup plus de services que ceux-ci, mais ceux-ci sont parmi les plus importants.

III. Concepts cryptographiques de base

Dans cette section, nous allons nous concentrer sur l'un des services de sécurité offert par la cryptographie, la confidentialité et en particulier, le mécanisme de sécurité du **chiffrement**. Nous allons examiner une différence critique entre la notion d'algorithme de chiffrement et de clé de chiffrement. Donc, à la fin de cette section, vous devriez être en mesure d'expliquer la différence entre un algorithme de chiffrement et une clé de chiffrement, et aussi, vous devriez être en mesure d'identifier deux types différents de cryptographie qui en résultent. Il pourrait être utile tout au long de notre discussion d'imaginer l'analogie de sécurité physique du chiffrement. Ce qui pourrait être, nous prenons en fait des informations écrites sur un morceau de papier, les plaçons dans une boîte et verrouillons cette boîte avec une clé. C'est en fait une analogie très utile pour ce que nous sommes sur le point de décrire.

Considérons donc maintenant une terminologie de base. Le **texte en clair** représentera donc les informations que nous essayons de protéger. Nous allons convertir cela, pour le rendre confidentiel, en quelque chose appelé **texte chiffré**, qui sera illisible et qui n'aura aucun sens.

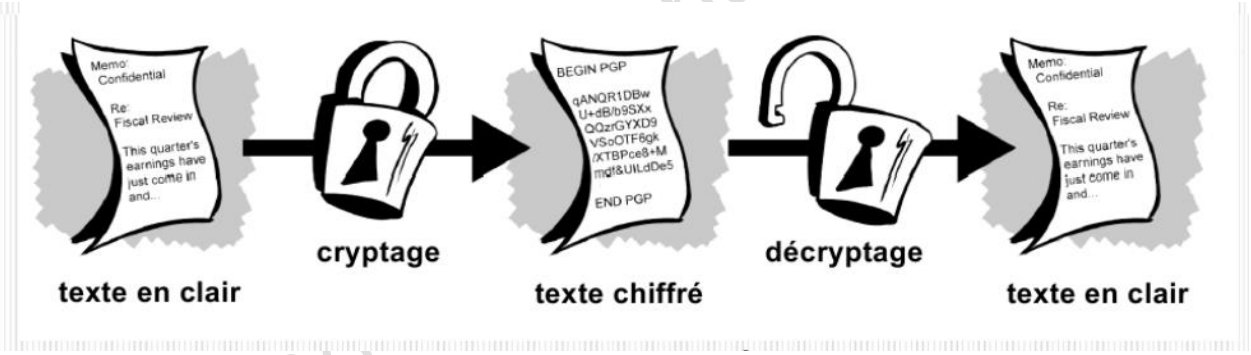


Figure 1 : Processus de cryptage et décryptage

Nous allons permettre à un attaquant d'observer le texte chiffré lorsqu'il est envoyé à travers un canal de communication et, espérons-le, il n'apprendra rien sur le texte en clair. La personne à qui nous envoyons les données, espérons-le, pourra d'une manière ou d'une autre récupérer le texte en clair à partir du texte chiffré. Voilà donc le **défi**. Maintenant, le moyen par lequel le texte en clair est converti en texte chiffré se fera au moyen d'un algorithme de chiffrement et un algorithme n'est en réalité qu'une recette. C'est donc un ensemble d'instructions qui disent brouiller le texte en clair de la manière suivante et le converti en texte chiffré. Puis l'algorithme de déchiffrement, connu du destinataire, lui permet de déconstruire ce texte chiffré et d'en récupérer le texte en clair.

C'est donc mieux vu au moyen d'un exemple, un exemple très, très simple et c'est quelque chose qui s'appelle le chiffre Atbash. Le chiffre Atbash est donc représenté par un tableau (figure au-dessous), il y

a des lettres en haut, des lettres en bas et nous cherchons simplement ce tableau pour convertir notre message en clair composé de lettres en haut, en un message chiffré composé de lettres bas et l'algorithme de chiffrement, dans ce cas, est très simple. Il dit simplement de rechercher le tableau et de remplacer la lettre en haut par la lettre en bas, et l'algorithme de déchiffrement est l'inverse. Par exemple le texte en clair "top secret" sera convertit en texte chiffrer "GLK HV XIVG", transmis a traves le canal de communication quand un attaquant le récupère il n`a pas vraiment de sens. Cependant, le destinataire, sachant que nous utilisons le chiffrement Atbash, peut déconstruire le message de la même table et récupérer le texte clair. La question est donc la suivante : obtenons-nous vraiment la confidentialité en utilisant chiffrement Atbash?

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	K	J	I	H	G	F	E	D	C	B	A

Figure 2 : Chiffrement Atbash sans clé

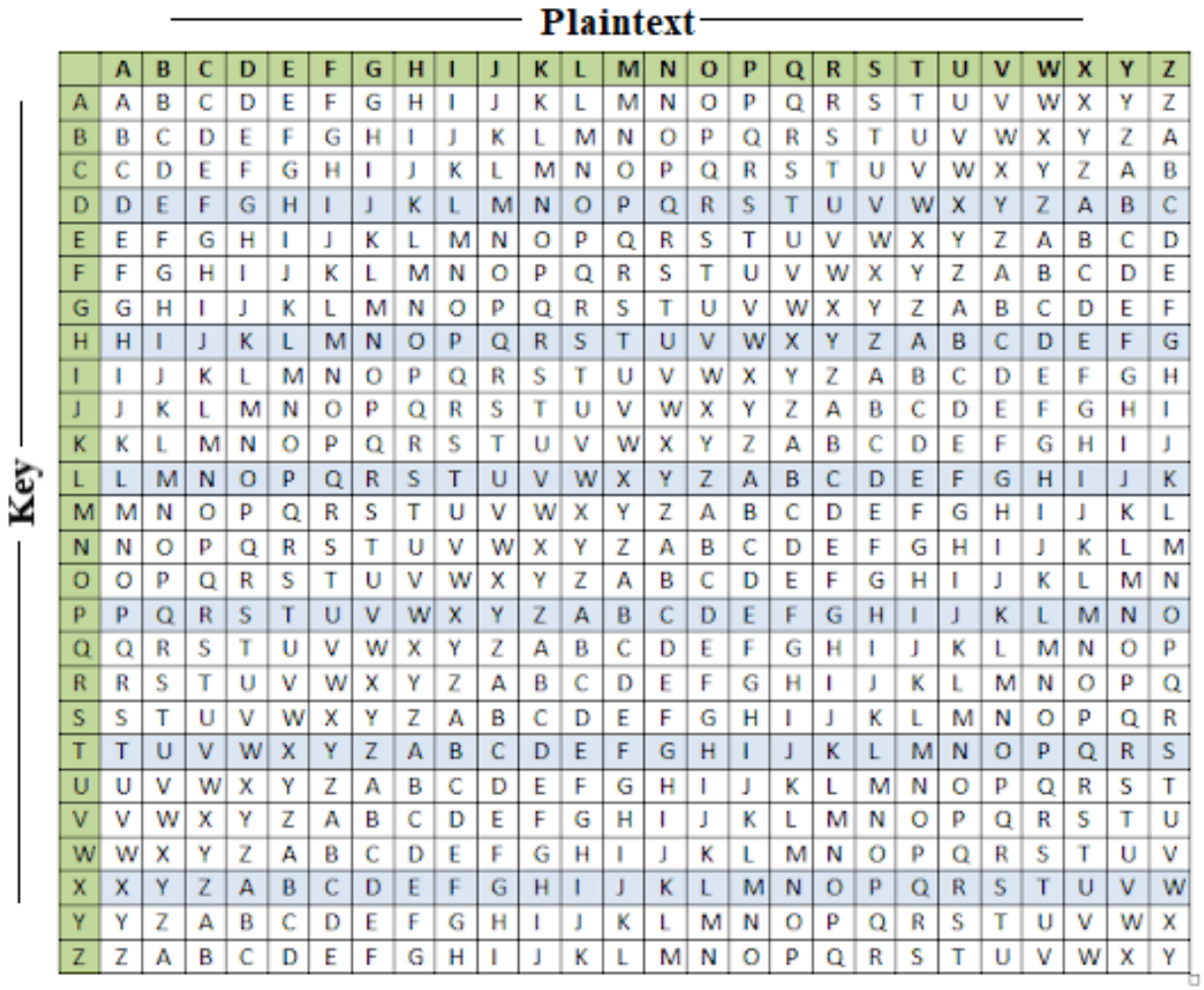
Eh bien, en fait, il y a de nombreuses raisons pour lesquelles la réponse est non, le chiffrement Atbash n'est pas un très bon moyen de brouiller les données. La plus fondamental, cependant, est que si vous pensez à la façon dont nous voulons utiliser la cryptographie dans les technologies modernes, il est important que tout le monde comprenne comment la sécurité est fournie. Si nous allons dire à quelqu'un que nous utilisons le chiffrement Atbash, alors en fait, nous révélons complètement comment nos données sont brouillées. Parce qu'il n'y a qu'un seul moyen dans le chiffrement Atbash de remplacer les lettres par des lettres. La lettre A est toujours remplacée par Z, la lettre B est toujours remplacée par Y, etc. Toute personne connaissant qu`en utilisant le chiffrement Atbash peut immédiatement récupérer un message. L'algorithme de déchiffrement est immédiat. Nous devons donc faire quelque chose d'un peu plus intelligent.

Clé de chiffrement

Maintenant, si nous revenons au modèle de chiffrement, ce que nous devons faire est d'introduire dans ce modèle quelque chose qui change et peut changer avec le temps et c'est le rôle d'une clé. Donc, encore une fois, pour convertir le texte en clair en texte chiffré, nous allons alimenter le texte en clair dans un algorithme de chiffrement, qui est une recette, mais qui va également prendre une clé de

chiffrement comme entrée et le texte chiffré produit dépendra non seulement de l'algorithme de chiffrement, mais également de la clé de chiffrement. De même, le destinataire aura besoin d'un algorithme de déchiffrement pour le déchiffrer. Mais ils auront également besoin d'une clé de déchiffrement, et c'est ce qui change avec le temps. Et encore une fois, cela est probablement mieux vu par un exemple.

Donc encore une fois, nous allons utiliser un algorithme de chiffrement qui est une table de recherche, nous allons échanger les lettres en haut par des lettres en dessous. Mais au lieu de n'avoir qu'une seule façon de le faire, nous allons faire en sorte que les lettres en dessous puissent être représentées de différentes manières. Ce qui va devoir se passer, c'est que l'expéditeur et le destinataire doivent se mettre d'accord sur la façon dont l'encodage est effectué. L'algorithme sera toujours une table, prenez la lettre en haut, remplacez-la par la lettre en dessous. Mais la lettre particulière choisie sera la clé, et cela sera inconnu d'un attaquant qui observe ce texte chiffré.



Key \ Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3 : Chiffrement Atbash avec clé

Vous pouvez voir que maintenant, il existe de nombreuses façons différentes de remplacer le texte clair par du texte chiffré et ils dépendent tous de différentes clés. Clés que le destinataire a convenues avec l'expéditeur avant l'utilisation du cryptage. Maintenant, en général, nous allons avoir besoin de beaucoup de clés. En fait, cette façon de chiffrer dont nous venons de parler est parfois appelée le **chiffrement par substitution**. La question est, de combien de façons différentes pourrions-nous avoir brouillé le message suivant "top secret" en utilisant le chiffrement par substitution ? La réponse est 40 000 fois plus que le nombre d'étoiles de notre univers, ce qui est beaucoup. Il n'y a donc aucun moyen pour quelqu'un de tenter sa chance sur la bonne clé dans ce type de système, s'il les essaie simplement au hasard. Maintenant, ce simple chiffrement de substitution est fondamentalement défectueux de nombreuses manières différentes, dont nous ne parlerons pas.

Ce qu'il est important de réaliser, c'est que les algorithmes de chiffrement modernes, comme **Advanced Encryption Standard**, qui est présent dans de nombreuses technologies que nous utilisons chaque jour, ne présentent pas ce genre de défauts. C'est en soi une recette, un moyen de brouiller les données. Un peu comme simplement remplacer la lettre en clair par le texte chiffré en dessous. C'est beaucoup plus compliqué, mais cela brouille les données d'une manière particulière, selon une recette particulière et cela prend aussi une clé, et il y a beaucoup, beaucoup plus de clés que même ce simple chiffrement de substitution. Mais il est fondamental de réaliser la différence entre la recette et la clé. Ce sont deux caractéristiques essentielles de tout processus de cryptage.

Il existe maintenant deux types de système de cryptage très différents, et c'est quelque chose qui mérite d'être signalé dès maintenant, si vous revenez en arrière et que vous vous souvenez que l'analogie avec le cryptage consiste à verrouiller les informations dans une boîte, il est en fait utile de penser aux verrous et aux clés pendant un moment. Parce qu'il existe deux types de mécanismes de verrouillage que nous utilisons dans le monde physique quotidien. Il y a des serrures où nous avons besoin de la même clé pour verrouiller une boîte, et nous avons besoin de cette clé pour déverrouiller la boîte, et nous avons besoin de la clé sur les deux parties du processus. Mais il y a aussi des clés, comme des cadenas, par exemple, où n'importe qui peut verrouiller la boîte simplement en fermant le cadenas, et seule la personne qui détient la clé peut déverrouiller la boîte et si nous pensons que le déverrouillage est un déchiffrement, ce que cela nous dit est dans n'importe quel mécanisme de chiffrement, la clé de déchiffrement devra être un secret. Il doit s'agir d'un élément détenu uniquement par le destinataire prévu de certaines informations. Mais la clé de verrouillage, la clé de chiffrement ne doit pas nécessairement être un secret et cela définit deux types de cryptographie.

Donc, dans la cryptographie symétrique, la clé de chiffrement et la clé de déchiffrement sont la même chose et par conséquent, doivent être secrets. Mais dans la cryptographie à clé publique, ou cryptographie asymétrique, un peu comme l'analogie avec le cadenas, la clé de cryptage peut être une

information publique. Ainsi, n'importe qui peut chiffrer quelque chose, et seule la clé de déchiffrement doit être un secret. Nous reviendrons sur l'importance de cela dans une section ultérieure, mais il est important à ce stade de réaliser que ces deux types de cryptographie très différents existent.

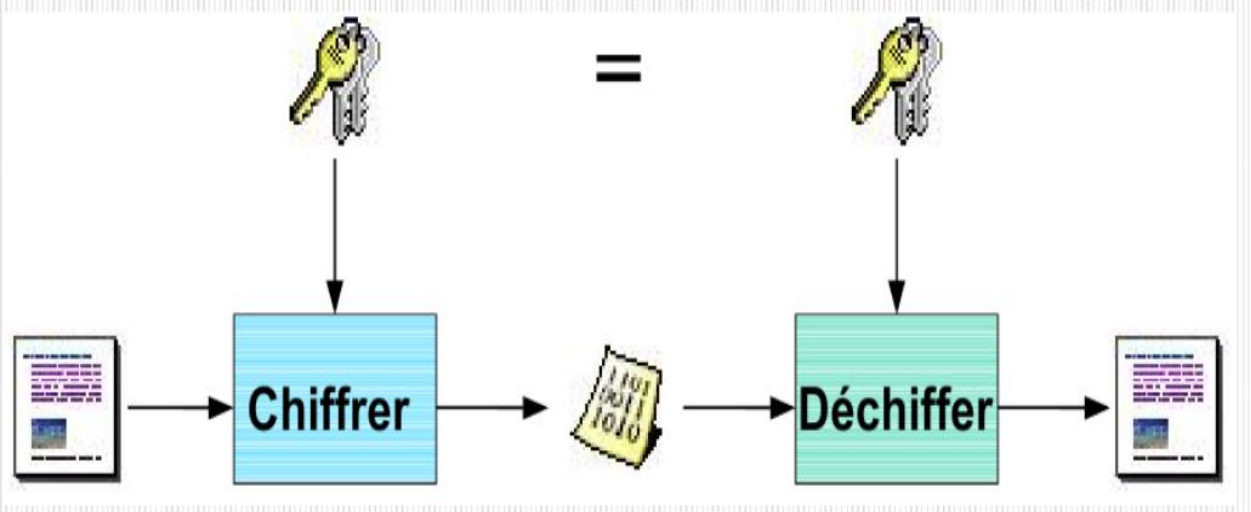


Figure 4 : cryptographie symétrique

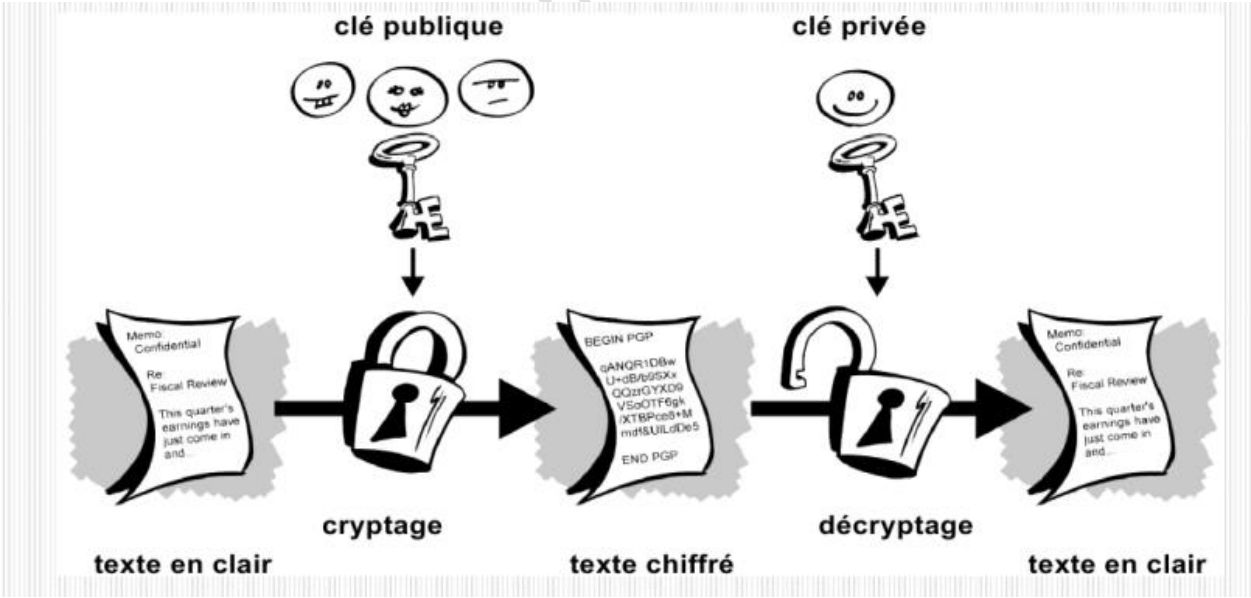


Figure 5 : Cryptographie à clé publique

IV. Points de faiblesse potentiels de tout système utilisant la cryptographie

Donc, dans cette section, nous allons examiner comment les cryptosystèmes pourraient être brisés. Cela peut sembler une chose étrange à faire, mais parfois la meilleure façon de comprendre quelque chose est de comprendre comment cela peut ne pas fonctionner. Ainsi, à la fin de cette section, vous serez en mesure d'apprécier que l'algorithme cryptographique ne soit qu'un composant d'un **cryptosystème** plus large et vous serez en mesure d'identifier les points de vulnérabilité potentiels dans un cryptosystème. Commençons donc par ce mot cryptosystème, qui est un nouveau mot que nous avons introduit et il est important de réaliser que dans la dernière section, nous avons parlé d'algorithmes et de clés. Mais dans le monde réel, l'algorithme n'existera pas de manière isolée.

Un algorithme cryptographique n'est qu'une partie du système plus large dans lequel il est implémenté. On peut donc penser à un cryptosystème comme étant constitué de l'algorithme. Mais aussi la façon dont il est mis en œuvre, la façon dont il est intégré dans la technologie pour laquelle nous voulons utiliser ce cryptosystème. Mais surtout, la façon dont les clés sont gérées. Les clés jouent un rôle très, très important dans la cryptographie, et elles doivent être entretenues et intégrées dans un système. La gestion des clés est donc un élément essentiel d'un cryptosystème. Il y a donc deux grandes façons de briser un cryptosystème au sens large et l'un serait, d'une manière ou d'une autre, d'accéder à la clé de déchiffrement, en quelque sorte de récupérer la clé de déchiffrement. Si vous pouvez le faire, tous les textes chiffrés produits à l'aide de la clé de chiffrement correspondante seront récupérables. Une alternative est en quelque sorte de trouver un moyen d'obtenir du texte en clair, sans cette clé de déchiffrement est si l'une de ces choses se produit, nous considérerons que le cryptosystème est cassé.

Commençons donc par le premier composant de ce cryptosystème, l'algorithme lui-même et une nouvelle alarmante, un algorithme peut toujours être cassé. Comment c’est ? Eh bien, considérons qu'un attaquant observe un texte chiffré qui a été brouillé et ils récupèrent le texte chiffré en écoutant le canal dans lequel il est envoyé. Cela n'a aucun sens pour eux. Mais ils connaissent l'algorithme qui a été utilisé, et c'est normal. Nous connaissons normalement l'algorithme utilisé pour produire du texte chiffré. Donc, s'ils connaissent l'algorithme, il y a toujours la possibilité d'essayer chaque clé de déchiffrement possible qui existe. Prenez la première clé de déchiffrement, essayez-la, déchiffrez le texte chiffré. Voyez si cela a du sens. Prenez la deuxième clé de déchiffrement, déchiffrez le texte chiffré, voyez si cela a du sens et continuez, et ce serait un processus très fatigant, espérons-le, à mener. est c'est pourquoi nous appelons cela une recherche clé exhaustive.

Vous obtenez de rechercher tout l'espace des clés de déchiffrement possibles. Nous venons donc de voir que chaque algorithme de chiffrement peut être brisé par cette recherche de clé exhaustive. Comment pourrions-nous empêcher cela ? Eh bien, la réponse est simple. Assurez-vous qu'il y a tellement de clés

de déchiffrement que ce n'est qu'une perte de temps pour quiconque et c'est exactement ce qui se passe. Dans tout algorithme de cryptage que nous utilisons dans la technologie moderne, il y a tellement de clés possibles qu'il est tout simplement irréaliste sur les ordinateurs modernes de rechercher toutes ces clés et de les trouver par accident. Donc, en fait, nous ne devrions pas vraiment nous inquiéter dans la cryptographie moderne de la recherche exhaustive de clés. Nous allons rendre cela impossible à réaliser dans la pratique.

Maintenant, si nous prenons de vrais algorithmes de chiffrement utilisés dans des produits vraiment commerciaux comme la norme de cryptage avancée. Il est probablement juste de supposer, en fait, que l'algorithme n'a pas vraiment de faiblesses. Pourquoi donc? Eh bien, la plupart des algorithmes de chiffrement modernes sont étudiés par des experts. Ils sont soumis à des panels de normalisation. Beaucoup de gens les ont regardés, analysés. Ils ne peuvent voir aucune faiblesse, cela ne veut pas dire qu'ils n'existent pas. Mais cela signifie que le genre d'expert de la croyance, c'est qu'il n'y a pas de faiblesses. Il serait donc raisonnable de supposer que dans une technologie moderne, normalement, on utilise un bon algorithme de cryptage, il y a tellement de clés qu'attaquer le cryptosystème au moyen de l'algorithme n'est pas réaliste.

Cependant, rappelez-vous que c'est un cryptosystème que nous pourrions attaquer, qu'il y a d'autres points faibles, l'un de ceux-ci est la mise en œuvre. Cet algorithme puissant doit être intégré à une véritable technologie et pendant la mise en œuvre, de nombreuses choses peuvent mal tourner. Quelqu'un pourrait ne pas suivre les instructions, les choses pourraient ne pas fonctionner comme prévu, les systèmes pourraient ne pas s'intégrer aussi bien que nous l'espérions.Donc il existe un certain nombre d'attaques de mise en œuvre subtiles contre les algorithmes de chiffrement modernes, notamment l'analyse de la consommation d'énergie lorsqu'un appareil effectue le chiffrement. Analyser la synchronisation pendant qu'un appareil effectue le chiffrement et voir si ces données elles-mêmes vous permettent d'obtenir des informations sur le texte en clair et les clés utilisées à ce moment-là. Donc, ceux-ci existent vraiment. et celles-ci sont appelées attaques par canal secondaire. Mais peut-être qu'une partie encore plus simple d'un cryptosystème à analyser est la gestion des clés. Et c'est l'un des points les plus faibles de tout cryptosystème, car les clés de chiffrements et les clés de déchiffrements doivent être réparties dans le système et prises en charge tout au long du fonctionnement du système. Ces clés doivent être créées., ils doivent être générés ils doivent être établis autour du réseau, aux bons endroits où ils sont nécessaires. Ils doivent être stockés en toute sécurité sur les appareils, quand leur vie est terminée, ils doivent être détruits.

Parfois, ils doivent être modifiés et toutes ces phases sont des phases où, en théorie du moins, un cryptosystème pourrait être faible, si l'une de ces étapes est exploitée. Il y a une autre partie d'un cryptosystème qui est très vulnérable, c'est une partie quelque peu évidente d'un cryptosystème, mais

c'est une partie que beaucoup de gens négligent est ce sont les points finaux. Pensez à acheter quelque chose en ligne, par exemple. Le texte en clair que vous souhaitez protéger ici sont généralement les coordonnées de votre carte bancaire. Normalement, nous chiffrons ce trafic au fur et à mesure qu'il traverse Internet, il arrive à la boutique en ligne, ils déchiffrent ces détails. Mais la question est : qu'advient-il des détails de la carte bancaire à chaque extrémité ? Où se trouvent vos coordonnées bancaires ? Les avez-vous mis dans un fichier sur votre ordinateur ? Sont-ils disponibles pour quelqu'un qui se trouve à côté de votre ordinateur et peut voir les détails de la carte ? et qu'advient-il des détails de la carte bancaire une fois que la boutique en ligne les a déchiffrés ? Que font-ils avec eux ? Parfois, nous ne savons pas. Il est important de réaliser que ces deux points de terminaison, où le texte en clair existe à la fois avant qu'il ne soit crypté et après son décryptage, sont des points vulnérables avec le cryptosystème sur lesquels nous devons nous concentrer.

Donc, en résumé, oui, les algorithmes de chiffrement sont des composants très cruciaux des cryptosystèmes, mais à bien des égards, ils sont la partie la moins susceptible d'être vulnérable d'un cryptosystème. Les faiblesses les plus courantes auxquelles nous pourrions nous attendre sont : l'implémentation, la gestion des clés et la gestion des données lorsqu'elles ne sont pas chiffrées, texte en clair, comment existe-t-il aux extrémités du système ?

V. Comment différents types de cryptographie sont utilisés dans les applications du monde réel

Dans cette section, nous allons examiner comment la cryptographie est utilisée dans des applications réelles. Encore une fois, nous allons nous concentrer sur le chiffrement. Nous allons vraiment de concentrer sur la façon dont le chiffrement est utilisé. À la fin de cette section, vous serez en mesure de reconnaître différents facteurs qui déterminent quand nous utilisons la cryptographie symétrique ou à clé publique et vous pourrez comparer la cryptographie utilisée dans plusieurs applications quotidiennes.

Commençons donc par récapituler. Il existe deux types de cryptage différents. Il y avait une cryptographie symétrique et une cryptographie à clé publique. En cryptographie symétrique, vous avez besoin de la même clé, de la même clé secrète pour chiffrer et déchiffrer et dans la cryptographie à clé publique, n'importe qui peut chiffrer et seul le destinataire peut déchiffrer. Maintenant, en fait, si vous y réfléchissez, l'un des gros problèmes que nous avons est de savoir comment les gens vont-ils obtenir les clés dont ils ont réellement besoin pour une application particulière. Maintenant, pour la cryptographie symétrique, l'expéditeur et le destinataire de toutes les données vont devoir s'entendre à l'avance sur un secret. Ce secret va être la clé. Alors que dans la cryptographie à clé publique, la clé de chiffrement peut être obtenue de n'importe où. C'est une connaissance publique et seule la clé de déchiffrement doit être gardée secrète. Donc, à première vue, il semble que la cryptographie à clé publique va sûrement être

bien meilleure. Ce sera beaucoup plus facile, car trouver les clés aux bons endroits du système sera sûrement un problème plus facile. La cryptographie symétrique est généralement très, très rapide. La cryptographie à clé publique implique peu de retards. Cela implique un travail de calcul difficile pour un ordinateur, donc c'est lent. En fait, malgré les avantages de la gestion des clés pour la cryptographie à clé publique, en général, nous ne voulons pas l'utiliser sauf si c'est nécessaire. Toute application de cryptographie essaiera vraiment d'être aussi symétrique que possible.

Jetons donc un coup d'œil à quelques applications quotidiennes qui utilisent la cryptographie symétrique et rappelez-vous que le problème est que nous devons organiser la présence d'une clé entre l'expéditeur et le destinataire avant de chiffrer quoi que ce soit. Mais il existe de nombreuses applications où cela est en fait assez simple. Le premier est donc votre téléphone portable. Donc, sur votre téléphone portable, il y a une carte à puce et sur cette carte à puce se trouve une clé. En revanche, la seule personne qui a besoin de le savoir est l'opérateur mobile avec lequel vous traitez. Ils doivent également connaître cette clé. Comment pouvons-nous faire en sorte que la même clé figure sur la carte à puce de votre téléphone et soit connue de l'opérateur mobile ? c'est simple, car c'est un opérateur mobile qui fait en sorte que la clé soit sur la carte à puce de votre téléphone. Donc, avant que vous n'obteniez réellement votre téléphone, et avant d'obtenir votre carte SIM, cette carte SIM a été connectée à l'opérateur mobile. Ils ont fait en sorte que la bonne clé soit mise en place.

Si vous le souhaitez, la clé a été établie avant même que vous ne mettiez la main sur l'appareil. Donc, dans ce cas, l'établissement de la clé, faire en sorte que la même clé soit sur la carte SIM comme avec l'entreprise de téléphonie mobile, était assez simple et il en va de même pour votre carte bancaire. Il y a une puce sur votre carte bancaire, sur cette puce se trouve une clé. La banque a besoin de connaître la clé. Comment est-ce arrivé ? Eh bien, vous avez votre carte de la banque, n'est-ce pas ? Donc, la clé a été préétablie si vous le souhaitez, sur la carte avant que vous ne l'ayez réellement. Encore une fois, l'établissement des clés est simple.

La cryptographie symétrique peut donc être utilisée. Pensons à une autre application qui utilise la cryptographie symétrique, votre réseau WiFi à la maison. Comment pouvons-nous organiser la distribution d'une clé de telle sorte que tous les appareils de votre maison puissent utiliser votre réseau WiFi? Eh bien, la réponse est probablement que vous l'avez fait. Ainsi, sur le routeur connecté à votre réseau WiFi, il y a des informations que vous avez probablement codées dans tous les appareils qui se connectent à ce réseau WiFi. Et c'était vous, en gros, en train de faire en sorte que la même clé soit connue de tous les appareils de votre maison qui se connectent à votre réseau WiFi. Ainsi, l'établissement clé dans cette situation était également simple. Par conséquent, la cryptographie symétrique peut être utilisée pour protéger le trafic envoyé sur tous ces canaux.

Considérons maintenant une application fondamentalement différente, c'est là que vous achetez quelque chose en ligne dans une boutique en ligne quelque part. Dans ce cas, une fois de plus, nous voulons crypter le trafic entre votre navigateur Web et la boutique en ligne sur laquelle vous souhaitez acheter quelque chose. Qu'est-ce qui est fondamentalement différent dans cet environnement ? Encore une fois, nous aimerions utiliser la cryptographie symétrique. Ce serait donc formidable si vous et la boutique en ligne aviez déjà convenu d'une clé. Mais vous ne l'avez pas fait, n'est-ce pas ? Il n'est pas possible de pré-convenir d'un secret avec une boutique en ligne, quelque part dans le monde où vous n'avez peut-être même jamais rien acheté dans le passé. Alors, comment contourner ce problème ? En fait, c'est exactement le type d'environnement où la cryptographie à clé publique est utile. Ainsi, dans ce cas, la boutique en ligne peut mettre à disposition une clé de cryptage publique que vous pouvez utiliser pour au moins commencer à utiliser la cryptographie pour protéger les communications. Parce que c'est un type d'environnement fondamentalement différent de ceux que nous avons examinés plus tôt. Donc, dans cet exemple d'achat de quelque chose dans une boutique en ligne, nous sommes obligés d'utiliser la cryptographie à clé publique d'une manière ou d'une autre. Mais nous savons également que la cryptographie à clé publique est plutôt lente. Alors pouvons-nous nous en sortir avec une utilisation chirurgicale juste pour ce dont nous avons besoin et pas plus que cela ? Et c'est ce qui se passe dans le protocole qui est souvent utilisé pour acheter des choses en ligne est quelque chose appelé SSL / TLS. Et cela fonctionne de différentes manières. Nous allons en décrire un maintenant.

C'est une façon de combiner la cryptographie symétrique et à clé publique pour obtenir le meilleur des deux mondes. L'idée est vraiment très simple. Essentiellement, vous souhaitez utiliser la cryptographie symétrique pour l'échange de données en masse. Les informations sur les détails de votre voiture, ce que vous achetez, tous ces détails. Nous voulons donc crypter cela de manière symétrique. Le problème est que votre navigateur et la boutique en ligne n'ont pas préalablement convenu d'une clé. Eh bien, ce qu'ils font, c'est pré-accepter la clé en utilisant la cryptographie à clé publique. Votre navigateur Web peut donc générer une clé symétrique. Cryptez cela à l'aide de la clé publique de la boutique en ligne. Transmettez cela à travers la boutique en ligne. Il récupère ou déchiffre ensuite pour obtenir cette clé symétrique. Maintenant, cette clé symétrique est utilisée pour chiffrer le trafic de données en masse. De cette façon, nous avons exploité le meilleur des deux mondes. Nous avons utilisé les merveilleuses propriétés de la cryptographie à clé publique pour crypter un message alors que nous n'avions jamais échangé de secrets à l'avance. Mais ce message est en fait une clé symétrique nous utilisons maintenant cette clé symétrique pour chiffrer le trafic en masse.

Donc, en résumé, nous avons examiné un certain nombre d'applications quotidiennes de la cryptographie. Nous avons vu que la plupart d'entre eux n'utilisent que la cryptographie symétrique et certains d'entre eux utilisent la cryptographie à clé publique pour échanger une clé symétrique puis une cryptographie symétrique pour protéger les données.

VI. Pourquoi le contrôle de la cryptographie présente une société avec une dilemme ?

Dans cette dernière section, nous allons faire quelque chose d'un peu différent et considérer réellement l'impact de la cryptographie sur la société. À la fin de cette section, vous serez en mesure d'expliquer pourquoi l'utilisation de la cryptographie pose un dilemme à la société et de comparer un certain nombre d'approches différentes pour résoudre ce dilemme de cryptographie. Ainsi, tout au long de nos discussions sur la cryptographie, nous avons supposé de manière générale que l'expéditeur et le destinataire qui échangent du trafic crypté sont de bonnes personnes et qu'ils cryptent leur texte en clair afin d'empêcher les mauvaises personnes de découvrir une sorte d'informations. Maintenant, il y a de nombreuses situations dans la société où cela est vrai, mais il y a de nombreuses situations où peut-être y a-t-il des nuances de gris. Il y a des situations dans lesquelles les personnes qui échangent des données cryptées peuvent bien faire quelque chose que les autorités souhaitent apprendre. Par exemple, les personnes enquêtant sur des activités criminelles ou pour des raisons de sécurité nationale. Si nous convertissons du texte en clair en texte chiffré de telle sorte que ce texte en clair ne puisse jamais être récupéré, alors nous présentons en fait un problème pour les enquêtes criminelles ou un problème pour la sécurité nationale parce que les informations échangées ne sont pas accessibles. Maintenant, ce problème existe depuis que la cryptographie a commencé à être utilisée dans un sens large. Mais depuis 2013, lorsque l'ancien sous-traitant de la National Security Agency **Edward Snowden** a commencé à informer le monde sur certaines pratiques des agences de renseignement du monde entier, nous avons commencé à apprendre que la cryptographie que nous utilisons chaque jour n'est peut-être pas aussi sûre que prévu. Maintenant, nous ne souhaitons pas porter de jugement sur ce qu'a fait Edward Snowden, ni même sur la moralité des activités de surveillance qui sont cryptées.

Ce que nous voulons faire maintenant, c'est simplement examiner les moyens par lesquels la cryptographie pourrait être sapée, si cela s'avérait nécessaire. Si vous y réfléchissez bien, presque toutes les techniques de rupture d'un système de cryptage pourraient être exploitées pour saper la protection offerte par la cryptographie. Vous pourriez miner l'algorithme, vous pourriez miner l'implémentation, ou vous pourriez en quelque sorte miner la gestion des clés. En fait, si nous repensons à l'histoire, nous verrons que presque toutes ces techniques ont été utilisées. En effet, un moyen de contrôler l'utilisation de la cryptographie dans les premières utilisations commerciales consistait à rendre l'algorithme moins puissant qu'il n'y paraît. Parfois, les algorithmes avaient ce qu'on appelait des "portes dérobées" qui rendaient l'algorithme moins puissant qu'il le devrait et le concepteur qui connaissait la porte dérobée pouvait peut-être récupérer des informations, récupérer une clé de déchiffrement, récupérer du texte en clair. Pour la personne utilisant l'algorithme, attendrait une protection complète de celui-ci. Une autre technique qui a été utilisée, au siècle dernier, par un certain nombre de pays du monde entier était d'imposer des contrôles à l'exportation sur la technologie cryptographique. C'était donc un moyen légal, dans un certain sens, de permettre l'utilisation d'un cryptage fort à l'intérieur des frontières d'un pays,

mais de restreindre la puissance du cryptage si cette technologie quittait ce pays. Ainsi, un produit pourrait être construit, un cryptage fort pourrait être utilisé à l'intérieur des frontières, mais si ce produit était vendu dans le monde entier, il aurait un cryptage plus faible. Désormais, placer une porte dérobée dans un algorithme de cryptage ou essayer de restreindre le mouvement du cryptage à travers les frontières sont en fait des techniques viables lorsque la cryptographie est intégrée dans des périphériques matériels. Un dispositif matériel doit quitter un pays et peut être inspecté à la frontière. Si vous allez affaiblir un algorithme d'une manière particulière, alors si c'est caché dans le matériel, peut-être que personne ne le remarquera. Mais dans les années 1990, nous avons commencé à voir apparaître des logiciels cryptographiques. La cryptographie était beaucoup plus couramment requise dans les logiciels, et aucune de ces techniques n'est très efficace. En effet, il y avait un différend dans le monde entier à propos de ce contrôle de la cryptographie, avec un certain nombre de cascades de haut niveau. Y compris les personnes imprimant du code cryptographique sur des t-shirts et errant à travers les frontières en portant leur cryptographie. Très difficile à aborder.

Ainsi, la dernière tentative radicale de modérer et de contrôler l'utilisation de la cryptographie à la fin des années 1990 était une idée appelée "Key Escrow". Cela a été suggéré par un certain nombre de gouvernements à travers le monde et l'idée de base était que tout le monde peut utiliser un cryptage fort, c'est très bien tant qu'une copie des clés de déchiffrements que vous utilisez est enregistrée auprès du gouvernement ou d'une autorité appropriée. Ils s'occuperont d'eux et en cas d'enquête criminelle ou d'incident de sécurité nationale, un tribunal pourra demander l'accès à la clé de déchifrement et le texte chiffré relatif à cette enquête pourra être déchiffré. En principe, cela semble être une bonne solution, mais si nous réfléchissons à la façon dont nous utilisons la cryptographie aujourd'hui par exemple dans nos cartes bancaires, WiFi, WhatsApp, toutes ces applications. Chaque fois que nous utilisons la cryptographie, ce système devra en quelque sorte être intégré à ce système, qui stocke en toute sécurité des copies des clés de déchiffrements, et n'importe quel homme d'affaires vous dira que cela va coûter cher, et un ingénieur vous le dira que cela ne fonctionnera probablement pas. En effet, Key Escrow a été fortement opposé en particulier par la communauté commerciale et il n'est jamais entré en vigueur.

Alors maintenant, regardons le monde moderne dans lequel nous vivons où la cryptographie est utilisée en permanence. C'est un monde complexe, de nombreuses applications, de nombreux réseaux. Beaucoup de cryptographie utilisée. Presque impossible de contrôler la cryptographie car elle est utilisée dans toutes ces différentes applications. La question qui se pose maintenant : est-il plus facile ou est-il plus difficile de contrôler la cryptographie dans ce monde moderne complexe ? Eh bien, dans le monde moderne est très compliquer, il est certainement difficile de mettre en place une sorte de contrôle général qui contrôle la cryptographie, probablement impossible. Mais dans toute la complexité du réseau moderne et l'utilisation moderne de la cryptographie, il existe de très nombreuses opportunités,

sans doute plus d'opportunités que par le passé, d'essayer en quelque sorte de saper la cryptographie, peut-être d'une manière désordonnée plutôt que d'une manière agréable et propre.

En fait, ce que nous avons vu d'après les révélations d'Edward Snowden et d'autres, c'est qu'il existe des preuves qu'une grande variété de techniques différentes sont utilisées aujourd'hui pour essayer de saper la cryptographie. Pensons simplement au genre de choses que vous pourriez faire. Par exemple, aujourd'hui, les téléphones portables sont des ordinateurs portables. Toutes sortes de données existent sur un téléphone mobile. Comment peut-on compromettre un téléphone mobile et accéder d'une manière ou d'une autre aux données cryptées? Eh bien, une technique relativement simple pourrait être de persuader l'utilisateur du téléphone de télécharger un code source informatique ou de télécharger une application sur son téléphone. Ce qui en fait est une application malveillante qui recherche d'une manière ou d'une autre des clés sur leurs téléphones, ou recherche un texte en clair sur leur téléphone et le signale. Maintenant que les utilisateurs de tous les téléphones ne sont pas des experts, vous pourrez peut-être cibler quelqu'un avec un tel logiciel malveillant.

Mais aussi les réseaux sont compliqués. Les données passent par toutes sortes de serveurs par toutes sortes de routes et n'importe où sur ces réseaux, partout sur ces réseaux les clés sont gérées, les clés sont distribuées, les clés sont stockées. Il existe de nombreux endroits autour de ces réseaux où les clés peuvent se cacher et parfois du texte en clair se cache et que l'un de ces endroits peut être visité si l'un de ces points est faible, c'est le point potentiel pour lequel une clé de déchiffrement pourrait fuir ou le texte en clair pu être trouvé. Cependant, les technologies sont compliquées, ils impliquent de vastes chaînes d'approvisionnement, différentes organisations dans différents pays fournissent différents composants. Il serait possible de compromettre un composant particulier provenant d'une sortie particulière. C'est un point de faiblesse possible car les systèmes sont compliqués. Par exemple, il est difficile d'obtenir les clés de tous les téléphones utilisés dans le monde. Il peut être possible d'obtenir les clés correspondant à un fournisseur particulier qui, pour une raison quelconque, a été compromis ou a décidé de coopérer avec une autorité qui souhaite accéder à ces clés. Le monde est donc compliqué, et dans cette complexité, il existe de très nombreuses opportunités différentes. Donc, dans un certain sens, en regardant en arrière, nous avons un dilemme. Nous aurons toujours un dilemme quelle que soit l'évolution de notre technologie. L'utilisation de la cryptographie nous posera toujours ce dilemme. Mais au fur et à mesure que le monde se complique et que nous utilisons de plus en plus de technologies de différentes manières, il existe de nombreux endroits dans les réseaux et les ordinateurs et les technologies que nous utilisons où la cryptographie peut faire du bon travail, mais pourrait également être compromise. C'est en son cœur le dilemme cryptographique qui ne disparaîtra pas de sitôt.

Donc, en résumé, l'utilisation de la cryptographie pose à la société un dilemme et ce dilemme au cœur est vraiment de savoir comment équilibrer la liberté et le contrôle dans la société moderne.