1. Introduction

Le **chiffrement des données est un enjeu majeur** de l'économie moderne. Sans elle il serait impossible de mettre en œuvre une économie globalisée.

1.1. L'exemple de l'envoi d'un mail

Lorsqu'un message électronique est envoyé, celui-ci transite par plusieurs serveurs avant d'arriver sur l'ordinateur du destinataire (figure 1).
Ce voyage n'est pas sans péril. En effet, ces serveurs appartiennent à des entreprises, des administrations ou des personnes peuvent ne pas s'embarrasser de scrupules et lire ce courriel.
Si le courriel n'est pas chiffré, c'est comme une carte postale sans enveloppe.

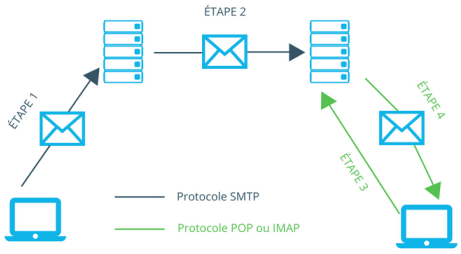

Fig 1 : parcours d'un courriel

Par exemple, en affichant le message détaillé d'un courriel (sous Gmail par exemple, cliquer sur « Afficher l'original », figure 2), le nombre de serveurs rencontré par le courriel est indiqué par le nombre de fois que le mot « Received » est cité.

Fig 2 : extrait du détail d'un courriel

2. Définitions

- **Cryptographie** : c'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.
- **Clé de chiffrement** : c'est un paramètre utilisé en entrée d'une opération cryptographique.
- **Coder** : représenter de l'information par un ensemble de signes prédéfinis. On utilise parfois le verbe encoder.
- **Décoder** : interpréter un ensemble de signes pour extraire l'information qu'ils représentent.
- **Chiffrer** : rendre une suite de symboles incompréhensible au moyen d'une clé de chiffrement.
- **Déchiffrer** : retrouver la suite de symboles originale à partir du message chiffré. On utilise le terme déchiffrer lorsque l'**on utilise une clé de déchiffrement pour récupérer le texte initial**.
- **Décrypter** : retrouver la suite de symboles originale à partir du message chiffré. On utilise le terme décrypter lorsque l'**on arrive à déterminer le message original sans utiliser la clé**.
- **Décrypter par force brute ou de manière exhaustive** : cela consiste à essayer toutes les clés possibles pour décrypter le message. Un des objectifs de la cryptographie moderne est de rendre cette méthode inefficace par un nombre toujours plus grand de clés possibles.

  Coder et décoder s'utilisent lorsqu'il n'y a pas de secret. Par exemple, on parle de "codage en complément à deux" des entiers. C'est juste une façon de représenter les entiers positifs ou négatifs par une suite de bits. N'importe qui peut décoder la suite de bits pour déterminer l'entier. Le terme "coder" (qui est un anglicisme, to code) est aussi utilisé de façon informelle comme synonyme de « programmer » comme dans la phrase "j'ai codé cette application". L'anglicisme "crypter" est à proscrire ; on utilisera "chiffrer".

3. La cryptologie

La **cryptologie** (la science du secret) repose sur la **cryptographie** (écriture secrète) et la **cryptanalyse** (analyse de cette dernière).

La cryptographie est pourtant une science très ancienne, on en trouve des traces 2 000 ans avant notre ère en Égypte ancienne.

Pour protéger les communications, on chiffre les messages à l'aide d'une méthode de cryptographie, comportant une ou plusieurs clés secrètes. Les deux principes de chiffrement sont le **chiffrement symétrique**, où la même clé est utilisée pour le chiffrement et le déchiffrement du message, et le **chiffrement asymétrique**, où deux clés différentes sont utilisées. Reste à assurer que les clés ne soient pas piratées, ce qui est le problème de l'authenticité des utilisateurs. La sécurité des communications dépend à la fois des méthodes de chiffrement et des protocoles d'échange des clés.

4. Chiffrement symétrique

4.1. Définition

Un chiffrement est dit symétrique si les clés de chiffrement et de déchiffrement sont identiques.

4.2. Fonctionnement

Dans le chiffrement symétrique, la clé dite partagée, est commune à l'ensemble des interlocuteurs. Elle est communiquée à l'ensemble de ceux-ci, par un moyen "sûr". Par exemple en rencontrant physiquement les interlocuteurs et en leurs donnant la clé sur un support amovible. Cette méthode reste peu pratique c'est pourquoi on utilise plutôt un système de cryptographie asymétrique pour diffuser cette clé.

Étape 1

Un ordinateur du réseau créé une clé et la diffuse à tous les ordinateurs qui doivent communiquer de manière sécurisée entre eux.

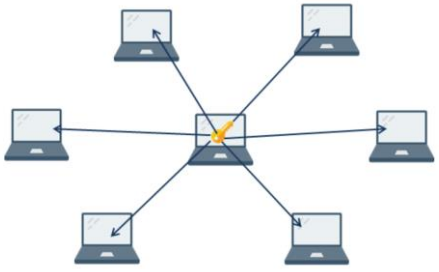

Fig 3 : création et diffusion de la clé

Étape 2

Chaque ordinateur du réseau stocke la clé partagée qu'il a reçu.

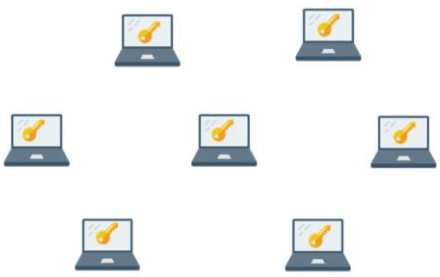

Fig 4 : stockage de la clé reçue

Étape 3

Communication chiffrée entre deux ordinateurs.

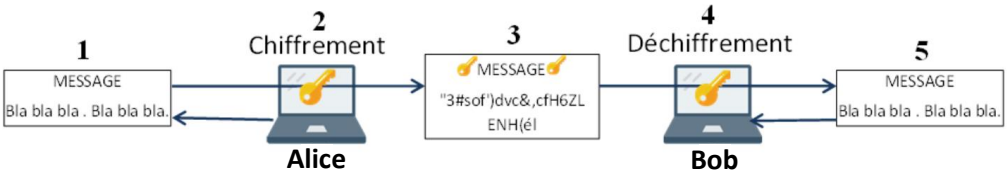

Fig 5 : communication chiffrée

1. Alice rédige son message en clair.
2. Alice utilise la clé partagée et chiffre son message.
3. Alice envoie son message chiffré à Bob.
4. Bob utilise la clé partagée pour déchiffrer le message.
5. Bob peut lire le message en clair.

4.3. Chiffre de César

Un des exemples le plus connu et le plus ancien de chiffrement symétrique est le chiffre de Jules César. Il consiste en un simple décalage des lettres dans l'alphabet, d'un nombre de lettres convenu à l'avance, la clé (figure 6).

Le chiffrement de César du message : HELLO WORLD avec une clé de 3 lettres (A est chiffré D, B est chiffré E…) donne le message chiffré : KHOOR ZRUOG

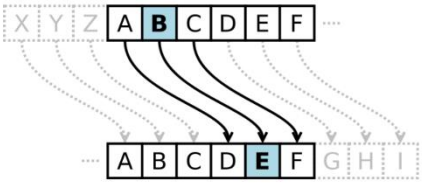

Fig 6 : principe du chiffrement de César

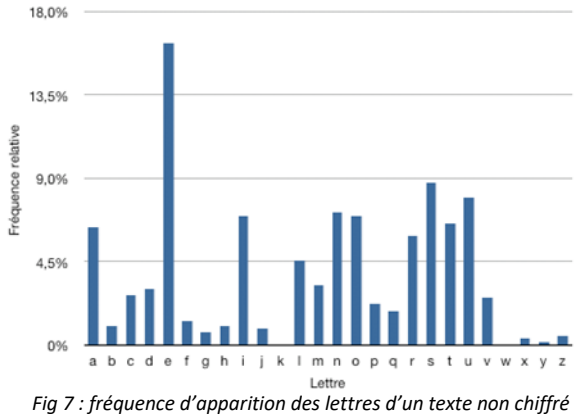

Fig 7 : fréquence d'apparition des lettres d'un texte non chiffré

Le code de César n'est pas très fiable car comme il ne comporte que 25 clés différentes (le décalage peut aller de 1 à 25), il est facile de le décrypter par force brute.

L'**analyse fréquentielle d'apparition des lettres** permet de trouver la clé rapidement.
À partir de cette analyse, on génère un graphique sur la fréquence d'apparition de chaque lettre dans le texte chiffré que l'on vient comparer à celle d'un texte non chiffré (figure 7). Le décalage entre les deux graphiques donne la clé de chiffrement.

4.4. Chiffre de Vigenère

L'idée de Blaise de Vigenère, diplomate Français (1523-1596), est d'utiliser le chiffrement de César, mais avec un **décalage différent suivant la position de la lettre** dans le texte ; la valeur de ce décalage est définie à l'aide d'une **clé**.

texte en clair	B	O	N	J	O	U	R	T	O	U	T	L	E	M	O	N	D	E
clé	N	E	N	U	P	H	A	R	N	E	N	U	P	H	A	R	N	E
décalage	13	4	13	20	15	7	0	17	13	4	13	20	15	7	0	17	13	4
texte chiffré	O	S	A	D	D	B	R	K	B	Y	G	F	T	T	O	E	Q	I

L'utilisation de plusieurs décalages différents rend **impossible l'analyse fréquentielle classique**. Cependant le chiffre de Vigenère a été cassé au 19ème siècle. **Il n'offre plus depuis cette époque aucune sécurité**. (https://fr.wikipedia.org/wiki/Cryptanalyse_du_chiffre_de_Vigen%C3%A8re).

4.5. Chiffrement XOR

Cette méthode repose sur l'opérateur logique XOR (ou exclusif), noté ⊕ et sur la répétition d'une clé alphanumérique.

Table de vérité de l'opérateur XOR entre deux bits E1 et E2 (ci-contre).

E1	E2	S
0	0	0
0	1	1
1	0	1
1	1	0

Propriété de XOR : soit trois nombres entiers x, y et z (codés sur 8 bits par exemple) tels que **x ⊕ y = z** alors on a aussi : **z ⊕ x = y** et **z ⊕ y = x**.

Soit le message **`Hello World!`** qui donne en binaire :
`01001000 01100101 01101100 01101100 01101111 00100000 01010111 01101111 01110010 01101100 01100100 00100001`
Chaque octet correspond au code ASCII de chaque caractère que l'on peut directement obtenir avec le site : https://www.rapidtables.com/convert/number/ascii-to-binary.html.

Soit le mot **`octet`** qui va servir de clé de chiffrement. Il donne en binaire :
`01101111 01100011 01110100 01100101 01110100`

Pour chiffrer le message, il faut effectuer un XOR bit à bit. Comme la clé est plus courte que le message, il faut "reproduire" la clé vers la droite autant de fois que nécessaire (si la taille du message n'est pas un multiple de la taille de la clé, on peut reproduire seulement quelques bits de la clé pour la fin du message).

```
  01001000 01100101 01101100 01101100 01101111 00100000 01010111 01101111 01110010 01101100 01100100 00100001
⊕ 01101111 01100011 01110100 01100101 01110100 01101111 01100011 01110100 01100101 01110100 01101111 01100011
  --------------------------------------------------------------------------------------------------------------
  00100111 00000110 00011000 00001001 00011011 01001111 00110100 00011011 00010111 00011000 00001011 01000010
```

Le code obtenu, en binaire, est :
`00100111 00000110 00011000 00001001 00011011 01001111 00110100 00011011 00010111 00011000 00001011 01000010`
Le message obtenu est alors : 'O4B

Le déchiffrement se fait à l'aide de la clé (**`octet`**) en réalisant à nouveau un XOR entre le message codé et la clé.

```
  00100111 00000110 00011000 00001001 00011011 01001111 00110100 00011011 00010111 00011000 00001011 01000010
⊕ 01101111 01100011 01110100 01100101 01110100 01101111 01100011 01110100 01100101 01110100 01101111 01100011
  --------------------------------------------------------------------------------------------------------------
  01001000 01100101 01101100 01101100 01101111 00100000 01010111 01101111 01110010 01101100 01100100 00100001
```

Après vérification le message décodé est bien : **`Hello World!`**

4.6. Data Encryption Standart (DES)

Le **Data Encryption Standard** est un algorithme de chiffrement symétrique utilisant des clés **de 56 bits**. Le premier standard du DES est sorti en 1977.
L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé. Avec une clé codée sur 56 bits, il peut exister 2^{56} = 7,2.10^{16} clés différentes.

Il est obsolète de nos jours à cause de la puissance des machines actuelles. Une recherche exhaustive ne prend que quelques heures avec des ordinateurs puissants.

4.7. Advanced Encryption Standart (AES)

Le Advanced Encryption Standard remplace actuellement le DES. **En cryptographie symétrique, il est actuellement le plus utilisé et le plus sécuritaire**. La clé a une taille de 128, 192 ou 256 bits.

Une utilisation connue du chiffrement AES est la clé WPA2 utilisée dans les réseaux WiFi.

4.8. Longueur de clé

En informatique, la **loi de Moore** implique que la puissance de calcul des processeurs disponibles sur le marché double tous les 15 à 24 mois, à coût constant. Cela signifie que l'on peut se doter de machines de plus en plus performantes pour attaquer les algorithmes de cryptographie. Il faut donc prendre la loi de Moore en compte lors du choix d'une longueur de clé : plus la durée de vie de la clé sera longue, plus il faut prendre une clé grande.
La courbe ci-contre montre que **dans les années 1980, une clé codée sur 56 bits garantissait une sécurité suffisante**, vu la puissance des ordinateurs. De nos jours, le standard est maintenant de 128 bits mais peut monter jusqu'à 4 096 bits.

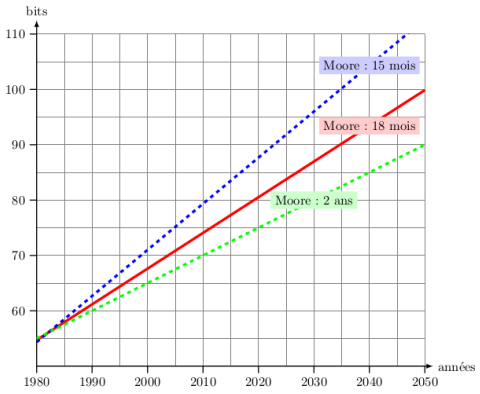

Fig 8 : nombre de bits nécessaires pour assurer une sécurité suffisante en cryptographie symétrique

5. Chiffrement asymétrique

5.1. Définition

Un chiffrement est dit asymétrique si les clés de chiffrement et de déchiffrement sont différentes.

Pour un chiffrement asymétrique l'une des clés est appelée **clé publique**, l'autre **clé privée**. La clé publique est diffusée sans chiffrage sur le réseau et peux être interceptée par un tiers (malveillant le plus souvent) sans que cela ne soit préjudiciable. La clé privée, quant à elle, est générée de différentes manières en fonction du système utilisé et ne sera jamais diffusée en clair sur le réseau.

Là encore, il existe de nombreux algorithmes de chiffrement asymétrique parmi lesquels on peut citer :

- Puzzles de Merkle (1974).
- Méthode de Diffie-Helman (1976).
- Le système RSA (Ronald Rivest, Adi Shamir et Leonard Adelman) (1977).

5.2. Principe de fonctionnement du système RSA

La clé publique dans ce système, est diffusée à tous les ordinateurs du réseau souhaitant communiquer avec celui qui l'a créé. La clé privée, quant à elle, reste sur la machine de son créateur.

Étape 1

Un ordinateur du réseau créé une clé publique et la diffuse à tous les ordinateurs qui doivent communiquer de manière sécurisée avec lui. Il créé aussi une clé privée qu'il conserve dans sa mémoire.

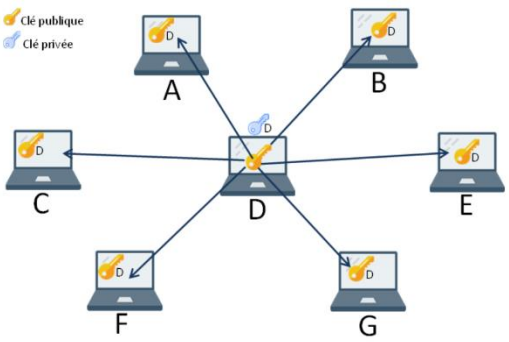

Fig 9 : diffusion de la clé publique

Étape 2

Lorsque chaque ordinateur du réseau a fait de même, toutes les machines sont en possession de nombreuses clés publiques et d'une seule clé privée (celle qu'il a généré lui-même).

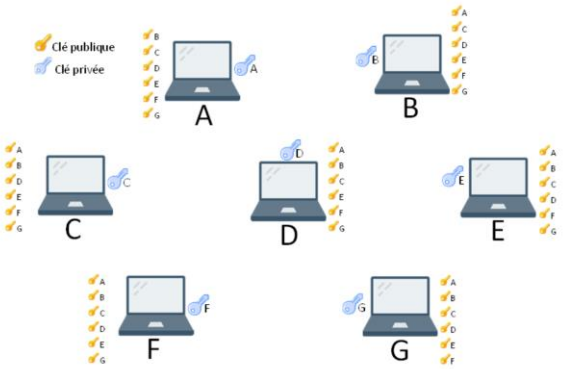

Fig 10 : clé privée et clés publiques

Étape 3

Envoi d'un message d'Alice à Bob. La clé publique sert à chiffrer un message et la clé privée à le déchiffrer.

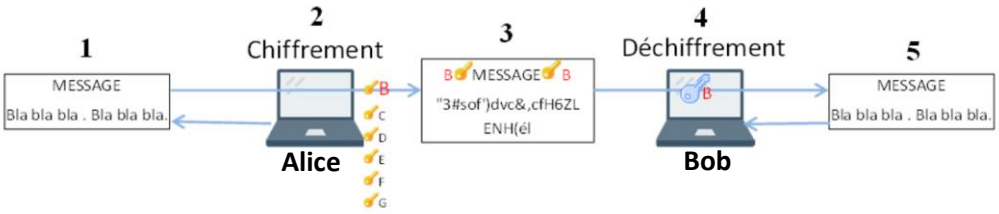

Fig 11 : communication chiffrée

1. Alice rédige son message en clair.
2. Alice utilise la clé publique de Bob pour chiffrer son message.
3. Alice envoie son message chiffré à Bob.
4. Bob utilise sa clé privée pour déchiffrer le message.
5. Bob peut lire le message en clair.

5.3. Limite du chiffrement asymétrique

Le chiffrement asymétrique étant beaucoup plus robuste que le chiffrement symétrique on peut être tenter de se passer de ce dernier. Cependant le chiffrement asymétrique reposant sur des calculs beaucoup plus complexes que ceux du chiffrement symétrique, il est beaucoup trop long de chiffrer l'intégralité d'un message par chiffrement asymétrique. On préfère donc, comme pour le protocole HTTPS, utiliser un chiffrement asymétrique pour diffuser de manière sécurisé une clé de chiffrement symétrique. Celle-ci est ensuite utilisée pour chiffrer les communications sans risque qu'elle soit utilisée par un tiers.

6. Alice et Bob

Les personnages **Alice et Bob** sont des figures classiques en cryptologie. Ces noms sont utilisés au lieu de « **personne A** » et « **personne B** » ; Alice et Bob cherchent dans la plupart des cas à communiquer de manière sécurisée.

Ces noms ont été inventés par **Ron Rivest** pour son article de 1978 dans le Communications of the ACM qui présentait le cryptosystème **RSA**.

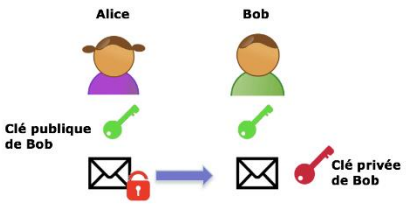

Fig 12 : personnage Alice et Bob

7. Loi française

L'usage de GPG (logiciel de chiffrement) a longtemps été interdit en France, car considéré jusqu'en 1996 comme une arme de guerre de deuxième catégorie. La législation française s'est ensuite assouplie, et le chiffrement symétrique avec des clés aussi grandes que 128 bits a été autorisé. **La loi pour la confiance dans l'économie numérique du 21 juin 2004 a totalement libéré l'utilisation des moyens de cryptologie**, en revanche leur importation ou exportation est soumise à déclaration ou autorisation. Ces démarches incombent au fournisseur du moyen de cryptologie et sont à accomplir auprès de **l'ANSSI**, **A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation.

7.1. Article de loi

L'Article 30-I rend l'utilisation des moyens de cryptologie libre.

> *L'utilisation des moyens de cryptologie est libre.*

Selon l'Article 434-15-2 du code pénal, le refus de remise de la clé de chiffrement entraine ceci :

> *Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.*
> *Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.*

Selon l'Article 132-79 du code pénal, l'utilisation d'un moyen chiffrement dans le but de commettre un délit peut engendrer une peine aggravante :
Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

> *1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ;*
> *2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle ;*
> *3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle ;*
> *4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ;*
> *5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement ;*
> *6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement ;*
> *7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.*
> *Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.*

Enfin selon l'Article 230-1 de la procédure Pénal, la justice peut se donner les moyens d'essayer de trouver les clés de déchiffrement.

> *Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.*
> *Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur de la République ou de la juridiction saisie de l'affaire le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Sauf si elles sont inscrites sur une liste prévue à l'article 157, les personnes ainsi désignées prêtent, par écrit, le serment prévu au premier alinéa de l'article 160.*
> *Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre.*