Université de Nice-Sophia Antipolis M1 Informatique
Cryptographie & sécurité 2016–2017

Examen de 6 juin 2017

Durée : 2h

Note :

Nom :
Prénom :

L'examen comporte quatres parties indépendantes. Répondez sur la copie avec clarté et concision.

1 Quizz sur la sécurité (5 points)

1. Pourquoi OpenSSL/TLS a besoin de la clé privée lors de la création d'un certificate signing request ?

   La biclé (pk, sk) est nécessaire pour garantir qu'on a bien la clé privée correspondant à la clé publique pour laquelle on demande la CSR

2. Expliquez ce qu'est une enveloppe digitale et quelle est son utilité.

   Une enveloppe digitale contient une clé secrète K chiffrée avec la clé publique du destinataire pk. Elle est utilisée pour transmettre K au propriétaire de pk

3. Quelle est la différence entre l'identification et l'authentification ?

   L'identification est l'affirmation d'une identité par son identifiant "Je suis Bruno". L'authentification apporte la preuve de l'affirmation d'identité

4. Comment peut-on transformer le calcul d'un MDC en un calcul de MAC ?

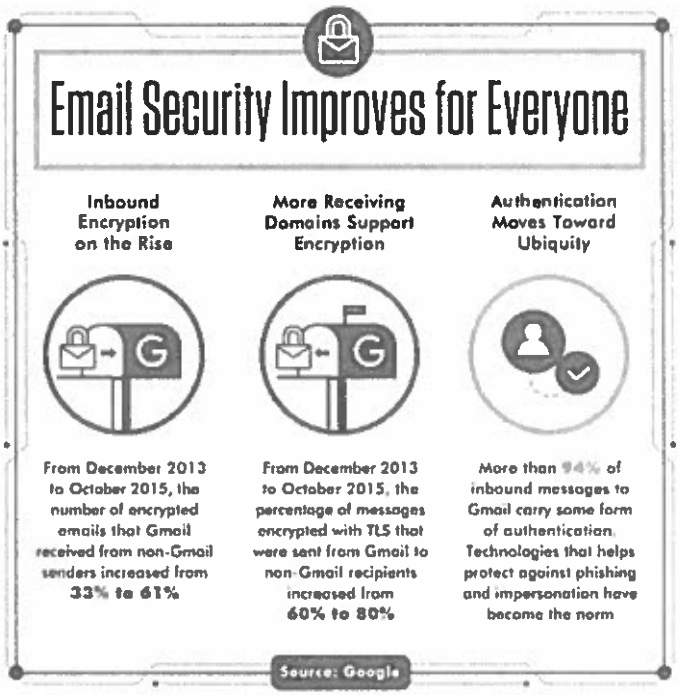
   Le MAC ajoute un service d'authentification. On peut transformer un MDC en MAC soit en prenant IV≠0 ou en ajoutant un paramètre en tête du msg fourni au MDC

5. A quoi sert un mécanisme de dérivation des clés ?

   A ne pas rejouer un protocole d'échange ou de mise en accord de clés. Une fois connue une clé partagée et un paramètre de dérivation on peut construire la future clé de session.

2 La sécurité du mail [5 points]

Un nombre croissant de sociétés (dont Google) cherchent à améliorer la sûreté du mail (voir l'infographie ci-dessous et consultez `http://g.co/saferemail`.



Avec vos connaissances en réseaux et en sécurité, commentez les affirmations de l'infographie :

1. Inboud encryption on the rise :

Cela signifie que smtpd accepte des connexions sécurisés par SSL/TLS pour le mail entrant (to:xxx@gmail.com) ⟺ le smtp de l'expéditeur utilise SSL/TLS

1

2. More receiving domains support encryption :

Cela signifie que les smtp destinataires supportent SSL/TLS. Un mail provenant de xxx@gmail.com peut être envoyé en l'encapsulant dans SSL/TLS

1

3. Authentication moves toward ubiquity :

Cela signifie que l'expéditeur peut être authentifié (surtout en utilisant les propriétés de DNSSec) ou par une autre mécanisme d'authentification

1

4. Expliquez en plus, les différences entre l'encapsulation du protocole `smtp` dans `TLS` ou `SSL` et le chiffrement du mail au moyen de `S/MIME` ou de `GPG`.

SSL/TLS chiffre les paquets qui voyagent depuis le smtp expéditeur vers le SMTP destinataire. Cela évite qu'ils soient interceptés (sniffés) lors de leur transport par le protocole smtp. Le fournisseur de mail a accès au contenu du mail GPG/PGP chiffre le corps du message envoyé par un expéditeur pour un destinataire spécifié. Cela fournit les services de confidentialité, intégrité et authentification. Seul le destinataire peut déchiffrer le message. Le fournisseur d'accès au service mail n'a pas accès au contenu.

1

5. Pensez-vous qu'il est utile de chiffrer les mails avec `S/MIME` ou `GPG` quand le protocole `smtp` est encapsulé dans `TLS` ou `SSL` ?

Pour les utilisateurs qui n'utilisent pas GPG, l'encapsulation du mail via smtp dans TLS offre une certaine confidentialité mais le fournisseur de mails peut lire le corps des messages. Pour garantir une parfaite confidentialité (+ auth et intégrité) il faut utiliser GPG avant transmission via smtp. L'encapsulation TLS va sûrement devenir un standard à terme.

1

3 Chiffre à clé secrète [5 points]

On considère un chiffre produit itéré à 3 tours dont les 3 fonctions de substitutions (boîte S) proviennent de trois chiffres définis par mot clé. Il chiffre des clairs de 9 lettres et fournit des chiffrés de 9 lettres.

1. Complétez chacune des 3 substitutions suivantes (S1, S2, S3) de l'alphabet des clairs dans l'alphabet des chiffrés pour chaque paire (`MOTCLE`, `lettre clé`) spécifiés :

S1 : (`MASTER`, `e`)

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

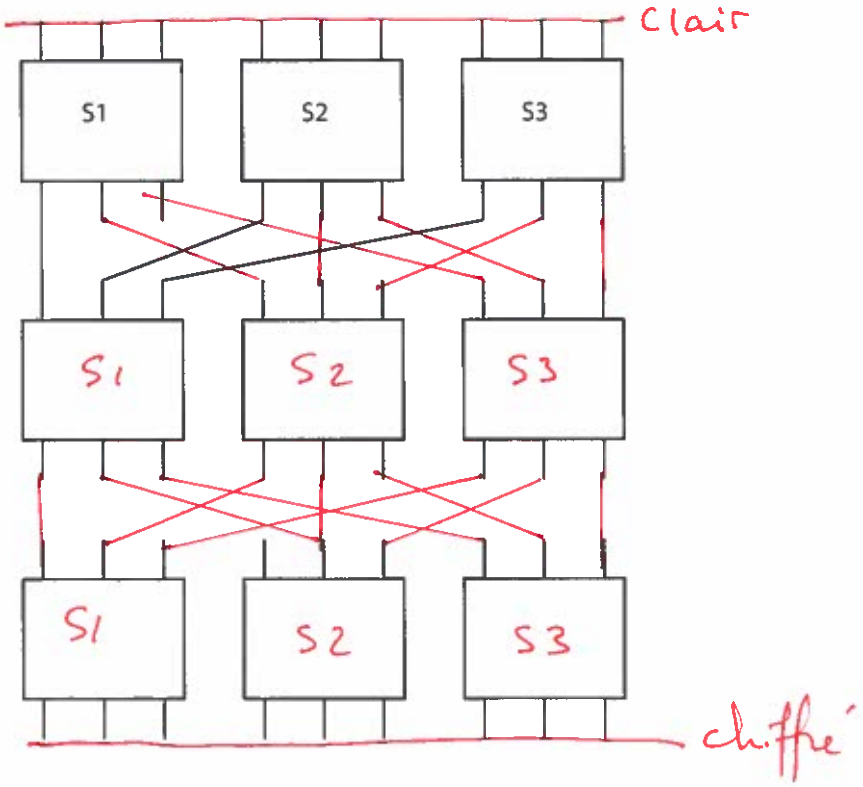
S2 : (`INFO`, `m`)

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

S3 : (`NICE`, `u`)

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

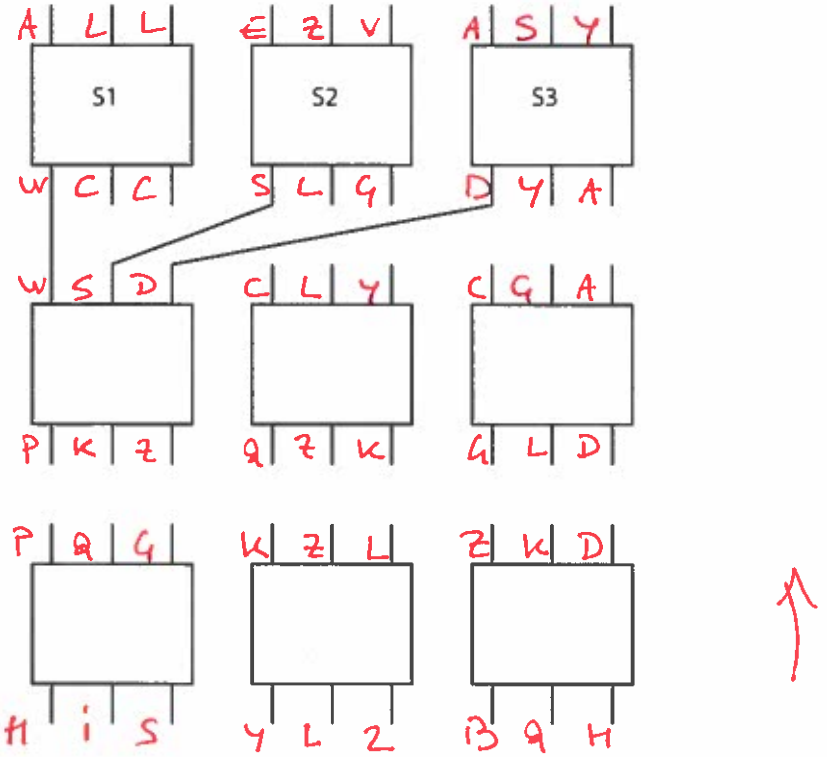
2. La transposition est obtenue en reliant la j^e sortie de la i^e boîte S à la i^e entrée de la j^e boite S du tour suivant. Complétez la suite de transpositions du chiffre sur le schéma suivant :



3. Expliquez comment déchiffrer un message.

En utilisant le dessin soit en passant le chiffré de haut en bas en calculant la bijection réciproque qui donne le clair ayant en le chiffré soit on fait passer le chiffré de bas en haut en cherchant la correspondance chiffré → clair dans chaque bijection

4. Déchiffrez le message `HIS YLZ BQH` en détaillant les opérations sur le schéma ci-dessous :



5. Dites ce que vous pensez de la sécurité de ce chiffre et donnez une amélioration simple et immédiate.

Amélioration immédiate : il n'y a pas de clé ! Il faut fournir une clé.

Sinon ce chiffre n'assure pas une très bonne sécurité car la permutation est connue. On doit pouvoir réaliser une cryptanalyse par analyse de fréquence (sauf si le mot clé est arbitraire et de la taille de l'alphabet)

4 OpenSSL [5 points]

1. Rappelez à quoi sert le protocole de Diffie-Hellman et dites pourquoi il est utilisé.

DH est un protocole mise en accord de clé (secrète).
Il est utilisé pour construire une clé secrète partagée entre
1 2 utilisateurs qui ne se sont pas rencontrés au préalable

Lors d'une connexion `OpenSSL`, le client et le serveur ont négocié les paramètres suivants : `DH-RSA-AES256-SHA256` qui sont autant de mécanismes de sécurité. Ils souhaitent communiquer en assurant les propriétés de sécurité suivantes :

- confidentialité ;
- intégrité ;
- authentification.

2. Après avoir donné le sens des acronymes, dites à quel(s) mécanisme(s) de sécurité correspond :

DH : mise en accord par Diffie-Hellman
RSA : chiffre à clé publique et signature : confidentialité, auth, intégrité
1 AES256 : chiffre à clé secrète de taille de bloc et clé 256 bits : confidentialité
SHA256 : fonction de hachage crypto sur 256 bits de sortie : intégrité

3. Si `RSA` est utilisé pour faire une enveloppe digitale dont le contenu est une suite de caractères ASCII, quelle est la taille maximale de la suite qui peut être chiffrée avec une clé de 1024 bits ?

1 caractère ASCII = 8 bits. On peut donc coder 1024 ÷ 8 = 128
caractères ASCII
1

`RSA` est plus sûr si on chiffre en utilisant g et h deux fonctions de hachage cryptographiques pour construire OAEP (pour Optimal Asymmetric Encryption Padding). Pour un clair M, une suite aléatoire r et g, h deux fonctions de hachage :

$$\mathrm{OAEP}(M) = \overbrace{(M \oplus g(r))}^{B_1}\|\overbrace{(r \oplus h(M \oplus g(r)))}^{B_2}$$

où $\|$ représente l'opération de concaténation et $\oplus$ l'opération du ou exclusif.

4 Expliquez comment on peut utiliser OAEP(M) pour chiffrer et pour déchiffrer avec RSA. On supposera connues les fonctions de hachage f et g ainsi que n, la taille de M.

Chaine de traitement $M \rightarrow OAEP(M) \rightarrow \{OAEP(M)\}_{pk_{RSA}}$
Pour déchiffrer, découper $\{\{OAEP(M)\}_{pk_{RSA}}\}_{sk} = OAEP(M)$ en B_1 de long. n et B_2
2 $r = h(B_1) \oplus B_2$
$M = B_1 \oplus g(r)$