Composition de Cryptographie – 2017/2018

Il est recommandé aux étudiants de bien choisir l'ordre des questions selon leurs compétences et rapidités.

Si l'élève n'arrive pas à faire une démonstration, il peut considérer que le résultat de la démonstration est admis sur le reste l'exercice.

Le support de cours et les calculatrices sont permis

1. Questions Courtes (maximum 2 lignes sauf là où est indiqué différemment)

a) Décrire une méthode d'échanger la clé de chiffrement dans un PKCS7-EncryptedData.
b) Quel est le padding utilisé dans une enveloppe PKCS7 utilisée pour la confidentialité ?
c) Quelle est l'utilité d'utiliser un salt et un nombre d'itérations dans PKCS5 ?
d) Alice veut transmettre un document signé à Bob avec une enveloppe PKCS7, mais inclure aussi un timestamp. Quelle zone sera affectée dans l'enveloppe PKCS7 ?
e) Alice veut transmette un document signé à Bob et Carole avec la même enveloppe PKCS7. Bob supporte le SHA256, et Carole le SHA1. Quelle solution préconisez-vous pour utiliser la même enveloppe et quelles zones seront impliquées ? (5 lignes maximum).

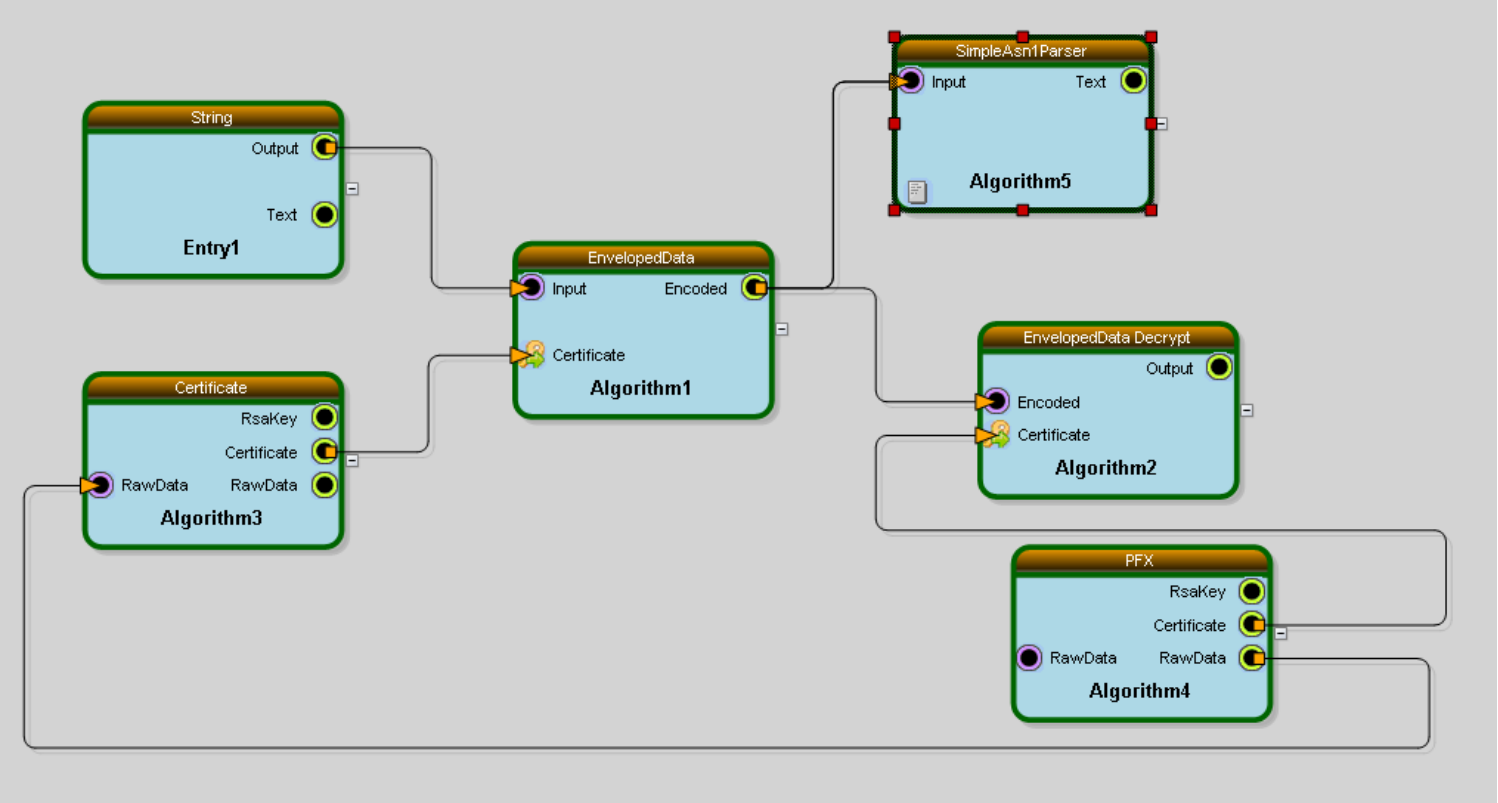
2. Clés RSA

Le but de cet exercice est d'analyser une attaque contre le RSA et améliorer la génération de clés RSA .
Le modulo N=p*q avec p < q ; p et q sont des nombres premiers. La taille de N est aux alentours de 2048 bits et que 2^{1023} < p et q < 2^{1025}
Le nombre p(x) de nombres premiers sur un intervalle [0..x] est de l'ordre de x/Ln(x) où Ln(x) est le log népérien de x.
Ln (2) = 0,69, Le nombre des habitants de la terre est de 6 Milliards = 3 * 2^{31}
Ln (x^{y}) = y * Ln (x)

a) Rappeler brièvement la génération d'une clé RSA.
b) Une autorité a généré deux clés ayant les modulos N1 et N2 avec la particularité suivante : N1 = p*q1 et N2= p*q2. Quel est le pgcd de N1 et N2 ?
c) A partir de la réponse suivante comment un attaquant peut déduire les clés privées connaissant uniquement N1, N2, et les exposants publiques P1 et P2 ?
d) A partir de l'attaque décrit précédemment, comment modifier la génération de clé RSA ?
e) Définir le nombre premiers pour les intervalles [0..2^{1023}] et [0..2^{1025}]. En déduire le nombre pour l'intervalle [2^{1023}..2^{1025}]
f) Nous allons que l'autorité ne génère plus de clés RSA pouvant être attaqué par l'attaque précédente. Définir le nombre de clés possibles. (Lemme du Berger).
g) Conclure sur la possibilité que chaque habitant de la terre peut oui ou non obtenir une clé RSA unique.

3. Schéma cryptographique

Soit le schéma



Le compte rendu est le suivant :

Algorithm1:Pkcs7

Variable	Value
Parameters	
Name	Algorithm1
Algorithm	Pkcs7
AlgorithmVersion	1.0(01)
OnError	Stop
Function	Enveloped
EncryptionAlgorithm	TripleDES
KeySize	128
Execution Results	
BeginTime	2018/04/13 13:54:26.327100
EndTime	2018/04/13 13:54:26.367100
ExecutionTime	00:00:00.0400000
ReturnCode	0

Input Values	
Certificate	[Subject] E=eaouad@easeit.fr, CN=E.AOUAD Encryption, O=EASEIT, L=Courbevoie, C=FR [Issuer] CN=EASEIT ROOT KEY 4096, OU=CRYPTOCENTER, O=EASEIT, L=Courbevoie, C=FR [Serial Number] 0EA4096000000006 [Not Before] 08/01/2009 19:26:15 [Not After] 29/10/2011 20:26:15 [Thumbprint] 201C2609B21C935B854FF40A7F8DA602FE2A7B89
Input	41 6C 69 63 65 20 61 75 20 50 61 79 73 20 64 65 73 20 6D 65 72 76 65 69 6C 6C 65 73
Output Values	
Encoded	30 82 01 F0 06 09 2A 86 48 86 F7 0D 01 07 03 A0 82 01 E1 30 82 01 DD 02 01 00 31 82 01 91 30 82 01 8D 02 01 00 30 75 30 69 31 0B 30 09 06 03 55 04 06 13 02 46 52 31 13 30 11 06 03 55 04 07 13 0A 43 6F 75 72 62 65 76 6F 69 65 31 0F 30 0D 06 03 55 04 0A 13 06 45 41 53 45 49 54 31 15 30 13 06 03 55 04 0B 13 0C 43 52 59 50 54 4F 43 45 4E 54 45 52 31 1D 30 1B 06 03 55 04 03 13 14 45 41 53 45 49 54 20 52 4F 4F 54 20 4B 45 59 20 34 30 39 36 02 08 0E A4 09 60 00 00 00 06 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 04 82 01 00 1D 32 9B E4 F3 B5 22 BC 33 D9 D4 26 47 8A 7A 7D 84 5E CF C4 6E 3F 1D FC 94 34 5D BB 02 16 30 E3 8C C4 8F E0 B2 8C 96 09 C2 52 49 5F BD DB 27 10 E4 8B F0 62 6E 55 D9 E9 F3 A2 19 DA 96 82 2E 55 10 1A FE CE FA BE 52 FF 09 6C 4F D0 4D 79 E1 88 E2 96 D9 AF D2 5E A9 63 14 28 27 35 6E A8 C0 E0 0E 0E AD 1D 3F E3 23 91 2D CB 56 46 36 0A 18 C2 31 50 04 52 59 9F A4 B7 32 8D 72 40 72 47 A1 21 F8 51 55 17 0C 90 5B C3 EB 6D D0 CE 8A 17 F5 3D 32 A2 76 A2 BA FE 0E CB F2 01 FE 3E A6 10 A9 95 87 93 57 89 79 00 B3 A7 35 BB 39 80 73 FA A7 3B 7E FB 53 78 50 7C 90 11 C8 61 74 C6 FF EC D9 EE 69 EB 0C E4 EB 5A 97 CC 00 6D 72 BD F4 5F 07 B4 1C F7 F6 79 8B 00 38 9C 4A 97 8D 0A 53 7E 36 6E EE 71 82 65 50 41 BA FA 7B 0C 1D AD 7C EA 22 F2 84 54 7B 15 1E DA 06 DA 71 4B 8B ED 65 CF 69 F6 30 43 06 09 2A 86 48 86 F7 0D 01 07 01 30 14 06 08 2A 86 48 86 F7 0D 03 07 04 08 34 4B 3F 18 2A E9 D1 C1 80 20 62 7E 8B 57 44 0C 1C E6 3F CD AF 78 6A 7D F2 91 61 74 ED 48 0A 74 5D ED D9 0B C3 21 D2 F6 58 CB
Output	null

La sortie de Asn1Paser est la suivante :

(0x30,0x000000,0x01F0) SEQUENCE
(0x06,0x000004,0x0009) OBJECT IDENTIFIER : envelopedData : '1.2.840.113549.1.7.3'
(0xA0,0x00000F,0x01E1) CONTEXT SPECIFIC (0)
(0x30,0x000013,0x01DD) SEQUENCE
(0x02,0x000017,0x0001) INTEGER : '0'
(0x31,0x00001A,0x0191) SET
(0x30,0x00001E,0x018D) SEQUENCE
(0x02,0x000022,0x0001) INTEGER : '0'
(0x30,0x000025,0x0075) SEQUENCE
(0x30,0x000027,0x0069) SEQUENCE
(0x31,0x000029,0x000B) SET
(0x30,0x00002B,0x0009) SEQUENCE
(0x06,0x00002D,0x0003) OBJECT IDENTIFIER :
countryName : '2.5.4.6'
(0x13,0x000032,0x0002) PRINTABLE STRING : 'FR'
(0x31,0x000036,0x0013) SET
(0x30,0x000038,0x0011) SEQUENCE
(0x06,0x00003A,0x0003) OBJECT IDENTIFIER :
localityName : '2.5.4.7'
(0x13,0x00003F,0x000A) PRINTABLE STRING :
'Courbevoie'
(0x31,0x00004B,0x000F) SET
(0x30,0x00004D,0x000D) SEQUENCE
(0x06,0x00004F,0x0003) OBJECT IDENTIFIER :
organizationName : '2.5.4.10'
(0x13,0x000054,0x0006) PRINTABLE STRING :
'EASEIT'
(0x31,0x00005C,0x0015) SET
(0x30,0x00005E,0x0013) SEQUENCE
(0x06,0x000060,0x0003) OBJECT IDENTIFIER :
organizationalUnitName : '2.5.4.11'
(0x13,0x000065,0x000C) PRINTABLE STRING :
'CRYPTOCENTER'
(0x31,0x000073,0x001D) SET
(0x30,0x000075,0x001B) SEQUENCE
(0x06,0x000077,0x0003) OBJECT IDENTIFIER :
commonName : '2.5.4.3'
(0x13,0x00007C,0x0014) PRINTABLE STRING :
'EASEIT ROOT KEY 4096'
(0x02,0x000092,0x0008) INTEGER : '0EA4096000000006'
u➔ (0x30,0x00009C,0x000D) SEQUENCE
(0x06,0x00009E,0x0009) OBJECT IDENTIFIER : rsaEncryption : '1.2.840.113549.1.1.1'
(0x05,0x0000A9,0x0000) NULL
v➔ (0x04,0x0000AB,0x0100) OCTET STRING :
'67673235AE4042A41B68410FBA10C168D79BB28F384FFF1F27AC2A0CCBB0CAB778F2706C6252700D2ABC38BB2FD1DD30EB6C19B54C19CB83
DB370C818977A5B7EC8D0B63B36DC13974AB7B224DBC384BDBFD8EA2A2FED243ED2F11C952FFA9882C82811F262CBF1781A8C426B0D18BDB
A2B0FE830AF84897C104F9E4D28B5ACF1CD57034372D6E22D3BFB4C2DBEAF43F31835A4512F2D774CB7018F84D57B614DD4745F0B5E46C204
FBF5AD64A24F04C494ADD3398B3B7EA178DBF1AC71DCFF7978ADB8EE1A7D6E3A71CB0B0D7A70A35C577439FBE5C4259C5C32D0E695CB9ED6
A6104A50FFC74D108A065E419226C9472149854709061684267C1B60E57159D'
(0x30,0x0001AF,0x0043) SEQUENCE
(0x06,0x0001B1,0x0009) OBJECT IDENTIFIER : data : '1.2.840.113549.1.7.1'
w➔ (0x30,0x0001BC,0x0014) SEQUENCE
(0x06,0x0001BE,0x0008) OBJECT IDENTIFIER : DES-EDE3-CBC : '1.2.840.113549.3.7'
x➔ (0x04,0x0001C8,0x0008) OCTET STRING : 'E277ED2392F44799'

y➔ (0x80,0x0001D2,0x0020) CONTEXT SPECIFIC (0) :
'F65F20946CE86B18E035D00F86170E36BA6E9CF43BE26C997C5DDD2967BAFD7E'

a) Interpréter le schéma.
b) A quoi correspond le certificat de l'entrée Certificate d'Algorithm1
c) Interpréter les champs u/v/w/x/y en gras de la sortie Asn1Parser
d) Si l'algorithme de chiffrement est AES quelle sera la taille du champs x ?

4. Sécurité IOT

Dans l'exercice le hub de données est de type serveur Raspberry.

a) Citez deux risques de sécurité liés à l'utilisation de hubs de capteurs dans une application IOT.
b) Citez deux limitations technologiques possibles liées à l'utilisation de hubs de capteurs.
c) Des hubs de capteurs de type Xbee (non programmables, onde radio) permettent d'utiliser un chiffrement AES avec une clé partagée entre tous les Xbee et le hub des données qui doit être aussi connecté à un Xbee récepteur. Quel service de sécurité primaire permet cette clé ?
d) Dans le cas précédent citez deux conséquences résultant de la divulgation du secret partagé.
e) On remplace les Xbee par des ESP32 (programmable comme arduino et communication wifi). Quel algorithme (non symétrique et non asymétrique) et son mode peuvent être utilisés pour faire l'authentification d'origine avec le hub des données?
f) Quelle variable unique de chaque l'ESP32 peut être utilisée pour permettre cette authentification ?
g) Comment l'algorithme en e peut être remplacé par un algorithme symétrique pour permettre l'authentification et la confidentialité ?
h) On désire augmenter le niveau de sécurité en utilisant les algorithmes asymétriques pour échanger des clés symétriques de session (chiffrement et déchiffrement de clé aléatoire).

A partir du tableau comparatif des tailles de clés équivalentes

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

et du tableau comparatif de quelques caractéristiques de l'ECC et RSA

Parameters	ECC	RSA

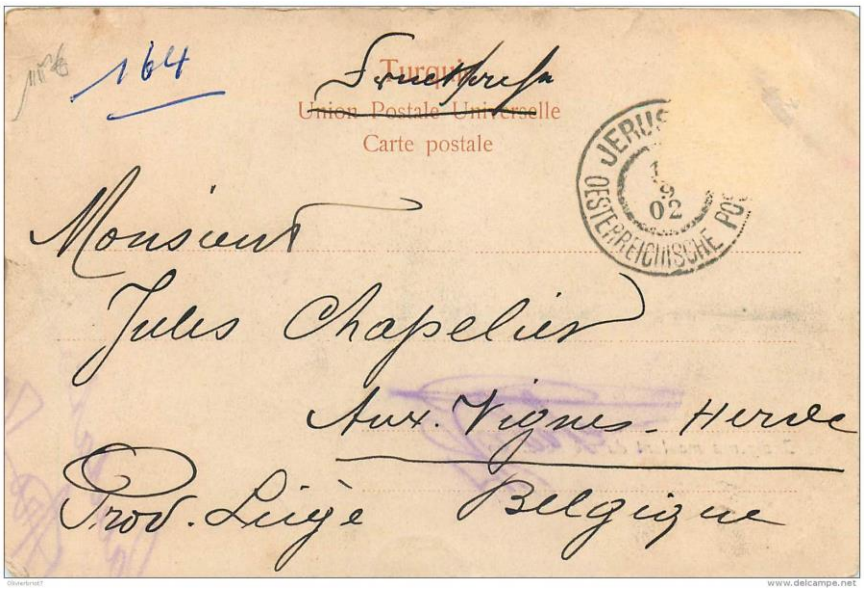
Bandwidth	saving ECC offers considerable bandwidth savings over RSA	Muc h less bandwidth saving than ECC
Encryption	Much Faster than RSA	At good speed but slower than ECC
Decryption	Slower than RSA	Faster than ECC

Pour quelles raisons préconisez-vous l'utilisation de l'ECC au lieu du RSA sur les ESP32 pour échanger des clés symétriques?

i) Pour quelle raison la vitesse de déchiffrement de clé symétrique n'est pas aussi importante que les raisons précédentes ?

5. Décryptage – Exercice Bonus

Soit la carte postale qui a été envoyée de Jerusalem en septembre 1902 en utilisant le bureau de poste autrichien. Le but de cet exercice est de décrypter le message que l'émetteur a écrit sur le recto de la carte. Le message peut contenir des fautes d'orthographe.



a) A partir de l'adresse du destinataire, déduire la langue probable du message.
b) Faire l'analyse spectrale des symboles.
c) En analysant les symboles : de quoi est formé chaque symbole ?
d) A quoi peut servir le point séparateur entre des ensembles de symboles
e) A partir de l'analyse spectrale, de la langue probable, et de la forme de chaque symbole, imaginer la table de correspondance entre l'alphabet et les symboles.
f) Mettre en équation la table précédente entre les caractères et les éléments des symboles.
g) Comment s'appelle le signataire du message ?
h) A partir de l'adresse du destinataire, pourquoi l'émetteur lui pose une question sur un pays ? (Note bonus liée à des connaissances générales)