Cryptographic Engineering

Important: This exam is composed of 4 parts:

Part 1: P. Karpman, **7 points**

Part 2: C. Pernet, **7 points**

Part 3: E. Peyre, **4 points**

Part 4: C. Ene, **6 points**

— Any manuscript document allowed

— Each of the 4 parts has to be answered on a separate answer sheet.

— The scale of grading is 24 points and your score over 24 will become your grade over 20. Hence it is not necessary to answer correctly all questions to get the maximum grade of 20.

— Your answers have to be short but clearly and cleanly argued or commented.

Part 1: Symmetric Cryptography (P. Karpman). 7 points

Exercise 1: The XEX tweakable block cipher construction

IND-CPA. We recall briefly and informally that an IND-CPA game is played in two phases. In a training phase, the Adversary has the possibility of sending query messages to the encryption scheme under analysis, and receives their encryption with some (fixed, a priori unknown, randomly picked) key. In a later challenge phase, the Adversary is tasked with deciding if an encrypted message c is an encryption of m_0 or an encryption of m_1, where m_0 and m_1 are two messages of its choosing of the same length; it wins the game if it makes a correct guess.

Let $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. The encryption of an l-block[1] message $m_1||m_2||\cdots||m_l$, $m_1, \ldots, m_l \in \{0,1\}^n$ with the "ECB" mode instantiated with E and a key k is defined as $E(k, m_1)||\, E(k, m_2)||\cdots||\, E(k, m_l)$.

Q.1

1. Show that the above ECB mode has poor security with respect to the IND-CPA definition, by exhibiting an efficient attack with a large advantage.

Let now $\widetilde{E} : \{0,1\}^\kappa \times \{0,1\}^\tau \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable block cipher. The encryption of an l-block message $m_1||m_2||\cdots||m_l$, $m_1, \ldots, m_l \in \{0,1\}^n$ with the "TIE" mode instantiated with $\widetilde{E}$ and a key k is defined as $\iota||\, \widetilde{E}(k, \iota, m_1)||\, \widetilde{E}(k, \iota+1, m_2)||\cdots||\, \widetilde{E}(k, \iota+(l-1), m_l)$, where $\iota \twoheadleftarrow \{0,1\}^\tau$.

Q.2

1. Explain informally why TIE is not vulnerable to your attack on ECB.
2. Suppose that the maximal length l of the messages is "small". What condition would you need to impose on τ in function of the total number N of messages that are to be encrypted with the TIE mode with a single key?

[1] For the sake of simplicity and without loss of generality, we assume here that all messages are made of an integral number of blocks.

⋆

We now define the XEX tweakable block cipher construction in the following way. Let E be as above, $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{2^n}^\times$, $\mathbb{I}_1, \ldots, \mathbb{I}_t \in \mathbb{Z}$, then $\mathsf{XEX}[E, \alpha_1, \ldots, \alpha_t, \mathbb{I}_1, \ldots, \mathbb{I}_t]$ is the tweakable block cipher $\widetilde{E} : \{0,1\}^\kappa \times (\mathbb{I}_1 \times \cdots \times \mathbb{I}_t) \times \{0,1\}^n \to \{0,1\}^n$ defined by $\widetilde{E}(k, i_1, \ldots, i_t, x) := E(k, x + \Delta) + \Delta$ where $\Delta := \alpha_1^{i_1} \cdots \alpha_t^{i_t} \cdot E(k, 0^n)$, with arithmetic being done in $\mathbb{F}_{2^n}$ and where 0^n stands for the string of n 0's.[2] The signature of $\widetilde{E}$ obtained thusly is different from the one used above in the TIE mode, but having such "'multi-dimensional" tweaks may be useful in some other modes of operation, especially authenticated-encryption modes. This however comes with the ***necessary security condition*** that for any fixed k the map $(i_1, \ldots, i_t) \mapsto \Delta$ be injective, i.e. $\alpha_1^{i_1} \cdots \alpha_t^{i_t} \cdot E(k, 0^n) = \alpha_1^{i'_1} \cdots \alpha_t^{i'_t} \cdot E(k, 0^n) \Rightarrow (i_1, \ldots, i_t) = (i'_1, \ldots, i'_t)$.

Finally, we will define $\mathbb{F}_2[X]/\langle P \rangle$ to be the field representation used for $\mathbb{F}_{2^n}$, with P some (a priori unspecified) polynomial of degree n irreducible over $\mathbb{F}_2$. Following usual conventions, we use 2 (resp. 3) to denote the class of X (resp. $X+1$) modulo P in this representation; in other words, a polynomial $Q = \sum_{i=0}^n q_i X^i \in \mathbb{F}_2[X]$ is represented by the integer $\sum_{i=0}^d q_i 2^i$.

Q.3

1. Why is it necessary in the XEX construction that $E(k, 0^n) \neq 0^n$?
2. Explain why $\Pr_{k \leftarrow \{0,1\}^\kappa}[E(k, 0^n) = 0^n]$ is negligible, assuming that E is a "good" PRP.

Q.4 We first focus on a case where $t = 1$, that is one has $\Delta := \alpha_1^{i_1} E(k, 0^n)$.

An irreducible polynomial P of degree n is said to be *primitive*, if the multiplicative order of 2 in $\mathbb{F}_2[X]/\langle P \rangle$ (i.e. the order of $2 \in (\mathbb{F}_2[X]/\langle P \rangle)^\times$) is equal to $2^n - 1$.

1. A user wishes to use $\alpha_1 = 2$. Explain why in this case it would be desirable that P be primitive.

Q.4 We now consider a case where $t = 2$ and P is primitive. A user would like to use $\alpha_1 = 2$ and $\alpha_2 = 3$, and wishes to find suitable values for $\mathbb{I}_1 = [\![-N_1, N_1]\!]$ and $\mathbb{I}_2 = [\![-N_2, N_2]\!]$ s.t. the map $(i_1, i_2) \mapsto \Delta$ is injective.

1. Assuming that $E(k, 0^n) \neq 0^n$, express the injectivity condition on $(i_1, i_2) \mapsto \Delta$ in terms of ℓ_3, the discrete logarithm of 3 in base 2.
2. Suppose that in some representation of some field $\mathbb{F}_{2^n}$, $\min_{x \in [\![-1000,1000]\!], x \neq 0}(|(x\ell_3 \mod 2^n - 1) - (2^n - 1)|) > 2^{117}$ (that is, there is no non-zero $x \in [\![-1000, 1000]\!]$ s.t. there is a reduction of $x\ell_3$ modulo $2^n - 1$ in the interval $[\![-(2^n - 2), 2^n - 2]\!]$ that is less than 2^{117} in absolute value. Or, put another way, $x\ell_3$ is at least "2^{117} far from 0" modulo $2^n - 1$). Propose (and justify) values for N_1 and N_2 that ensure injectivity.
3. Would the computation of ℓ_3 be tractable in $\mathbb{F}_{2^{128}}$ (N.B.: Note that the largest prime factor of $2^{128} - 1$ is $67280421310721 \approx 2^{46}$)?

Q.5 One can show that $\mathbf{Adv}^{\widetilde{\mathrm{SPRP}}}_{\widetilde{E}}(t, q) \leq \mathbf{Adv}^{\mathrm{SPRP}}_{E}(t', 2q) + \mathcal{O}(q^2)/2^n$, where $\widetilde{\mathrm{SPRP}}$ is the relevant adaptation of the SPRP security definition to tweakable block ciphers, and with $t' \approx t$ in practice.

1. Do you think that a tweakable block cipher built with an XEX construction could be used in a "beyond-birthday bound" mode of operation?

⋆

N.B.: This exercise is based on the paper *Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC*, Phillip Rogaway, ASIACRYPT 2004.

[2] This in fact slightly simplifies over the original XEX construction which also allows $E(k, 0^n)$ to vary.

Part 2: Asymmetric Cryptography (C. Pernet). 7 points

Exercise 2: Reductions

Among the following computational problems:
`BreakRSA`: From $(n = pq, e)$ find d such that $ed = 1 \mod \varphi(n)$
`CDH`: From $A = g^a$ and $B = g^b$ in a group, find $C = g^{ab}$
`DLOG`: From (g, g^x) from a group G find $x \in \{1, \ldots, |G|\}$.
`ModExp`: From (x, n, e) integers compute $x^e \mod n$
`IntegerFact`: From $n = pq$ an integer, find p and q

1. List 4 reductions in the form `ProblembA` $\leq$ `ProblemB`.
2. For two of them of your choice, explain the outline of the proof: which supposition is made at the beginning and which conclusion is reached (you don't have to actually prove it).

Exercise 3: Coding Theory

Consider the following tuples of code parameters of the form (n, k, d), where n is the length, k the dimension and d the minimum distance:
(a) $(24, 10, 2)$ over $\mathbb{F}_{256}$
(b) $(32, 11, 22)$ over $\mathbb{F}_{32}$
(c) $(8, 5, 3)$ over $\mathbb{Z}/11\mathbb{Z}$
(d) $(10, 6, 4)$ over $\mathbb{Z}/2\mathbb{Z}$
(e) $(12, 8, 5)$ over $\mathbb{Z}/19\mathbb{Z}$

1. Which one has the largest information rate?
2. Which one can correct the largest number of errors?
3. For each of them, say whether or not it can be achieved by a Reed-Solomon code. Justify your answers.
4. For a set of parameters which can be achieved by a Reed-Solomon code, explain how to construct such a Reed-Solomon code : definition of the code, and describe an encoding algorithm, and a decoding algorithm.

Part 3: Elliptic curves (E. Peyre). 4 points

Exercise 4: Elliptic curves

Let E be the elliptic curve defined by the affine equation

$$Y^2 = X^3 - X + 1$$

over $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$.

1. Check that E is smooth.
2. Give the list of elements in $E(\mathbb{F}_7)$.
3. Find all points of order 2 in $E(\mathbb{F}_7)$.
4. Is the group $E(\mathbb{F}_7)$ cyclic?

Part 4: Models and analysis of security protocols. 6 points

Exercise 5 (2 pts.)

In this exercise, $\langle \_ , \_ \rangle$ represents concatenation, $[\ \_\ ]\_$ represents a symmetric encryption scheme, $\{\ \_\ \}\_$ an asymmetric encryption scheme, and $pr(u)$ is the inverse secret key associated to $pk(u)$. We recall the rules of the Deduction System for Dolev Yao theory that allows (by repeted application) to infer a term t from a set of terms T_0 (denoted $T_0 \vdash t$):

$$\textbf{(A)}\ \frac{u \in T_0}{T_0 \vdash u} \qquad \textbf{(UL)}\ \frac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u} \qquad \textbf{(C)}\ \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash [\ u\ ]_v} \qquad \textbf{(AC)}\ \frac{T_0 \vdash u \quad T_0 \vdash pk(v)}{T_0 \vdash \{\ u\ \}_{pk(v)}}$$

$$\textbf{(P)}\ \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v\rangle} \qquad \textbf{(UR)}\ \frac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash v} \qquad \textbf{(D)}\ \frac{T_0 \vdash [\ u\ ]_v \quad T_0 \vdash v}{T_0 \vdash u} \qquad \textbf{(AD)}\ \frac{T_0 \vdash \{\ u\ \}_{pk(v)} \quad T_0 \vdash pr(v)}{T_0 \vdash u}$$

The set of **Syntactic Subterms** of a term t, denoted by $S(t)$, is the smallest set such that:

— $t \in S(t)$

— $\langle u, v\rangle \in S(t) \Rightarrow u, v \in S(t)$

— $[\ u\ ]_v \in S(t) \Rightarrow u, v \in S(t)$

For a set T of terms, we define $S(T) = \bigcup_{t\in T} S(t)$.

The following algorithm allows to decide if $T_0 \vdash w$ (where $T \vdash^{\leq 1} s$ means that s can be obtained from T using only one rule from the Deduction System):

McAllester's Algorithm

Input : T_0, w

$T \leftarrow T_0$;

while $(\exists s \in S(T_0 \cup \{w\})$ such that $T \vdash^{\leq 1} s$ and $s \notin T)$

$T \leftarrow T \cup \{s\}$;

Output :$w \in T$

1. Using the above algorithm, prove or disprove that a passive Dolev Yao intruder can deduce the message s with the initial knowledge T_0.

   1.) $T_0 = \{a, k, n1, [\ s\ ]_{\langle n1,n5\rangle}, [\ s\ ]_{\langle n2,n4\rangle}, [\ n3\ ]_{\langle n2,n1\rangle}, [\ \langle n4, [\ n3\ ]_{\langle n4,n1\rangle}\rangle\ ]_k, [\ \langle k1, [\ n2\ ]_{\langle n4,n1\rangle}\rangle\ ]_{n3}, [\ n2\ ]_{n5}\}$

   2.) $T_0 = \{a, b, [\ k1\ ]_{k2}, k2, [\ s\ ]_{\langle k3,k1\rangle}, [\ k4\ ]_{\langle k1,k2\rangle}, [\ \langle [\ s\ ]_{k3}, [\ s\ ]_{k6}\rangle\ ]_{k5}, [\ \langle [\ k6\ ]_{k1}, [\ k1\ ]_{k5}\rangle\ ]_{k2}, [\ [\ k4\ ]_{k3}\ ]_{k1}\}$.

2. We add to the Dole-Yao inference system given above a new rule corresponding to block encryption modes such as ECB (Electronic codebook) or CBC (Cipher-block chaining).

   $$\textbf{(ECB)}\ \frac{T_0 \vdash [\ \langle u, v\rangle\ ]_w}{T_0 \vdash [\ u\ ]_w}$$

   It reflects the fact that an attacker may compute the prefix of an encrypted message (provided the length of the prefix is a multiple of the length of a block). Can you extend the notion of **Syntactic Subterms of a term** t to some different notion of **Semantic Subterms of a term** t **(denoted also** $S(t)$**)** such that the McAllester's Algorithm remains sound with respect to the deducibility of a message w from a set of terms T_0?

Exercise 6 (2 pts.)

In this exercise, $\langle \_ , \_ \rangle$ represents concatenation, $[\ \_\ ]\_$ represents a symmetric encryption scheme, $\{\ \_\ \}\_$ an asymmetric encryption scheme, $pk(u)$ is the public key associated to the user with identity u and $\oplus$ denotes the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$. Consider the following protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B \quad : \{\ \langle \langle A, B\rangle, N_a\rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A \quad : \langle \{\ \langle K, N_b\rangle\ \}_{pk(A)}, [\ N_a \oplus B\ ]_K\rangle \\ 3. & A & \rightarrow & B \quad : \{\ \langle \langle A, N_b\rangle, K\rangle\ \}_{pk(B)} \end{array}$$

The goal of this protocol is to provide both secrecy and authentication: at the end of a session between two honest participants a and b, k (the instantiation of the parameter K in the specification of the protocol) should be a new shared secret value known only by a and b. This target session

between honest participants a and b may be part of a richer scenario containing other running sessions in parallel where the active adversary i can be involved. If you think that the protocol is correct, then give a justification. Otherwise,

— give an attack on the target session between honest participants a and b where the intruder i will learn k;

— propose a correction of the protocol.

Exercise 7 (2 pts.)

In this exercise, $\langle \_, \_ \rangle$ represents concatenation, $\{\ \_\ \}_\_$ represents an asymmetric encryption scheme, and $pk(u)$ is the public key associated to the user with identity u. All protocols in this exercise are intended to provide acknowledgement of the receipt of an encrypted message m by the intended receiver b, i.e. at the end of a session between honest participants a and b, a will think that she is talking to b and she is sharing a secret value m with b. For all following protocols, you should consider a target session between honest (uncorrupted) participants a and b, part of a richer scenario containing maybe other running sessions, and check if m (the instantiation of variable M in this session) remains secret in presence of an active Dolev-Yao intruder. For all protocols below, if you think that the protocol is not correct, give an attack on the target session between honest participants a and b where the intruder i will learn m (maybe using other sessions running in parallel where i can be involved), but if you think that the protocol is correct, pthen give a justification.

1. We start with a naive protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B \quad : \langle A, \{\ M\ \}_{pk(B)} \rangle \\ 2. & B & \rightarrow & A \quad : \{\ M\ \}_{pk(A)} \end{array}$$

2. A more "elaborate" protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B \quad : \{\ \langle A, M \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A \quad : \{\ M\ \}_{pk(A)} \end{array}$$

3. And a "very encrypted" protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B \quad : \{\ \langle A, \{\ M\ \}_{pk(B)} \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A \quad : \{\ M\ \}_{pk(A)} \end{array}$$