Cryptography and Security — Midterm Exam

Serge Vaudenay

9.12.2016

- duration: 1h45
- no documents allowed, except one 2-sided sheet of handwritten notes
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will <u>**not**</u> answer any technical question during the exam
- readability and style of writing will be part of the grade
- answers should not be written with a pencil

1 An Attempt to Fix Double Encryption

We consider a block cipher C over n-bit blocks with a key of n bits. We define $\mathsf{Enc}_{K_1,K_2,K_3}(x) = C_{K_3}(C_{K_1}(x) \oplus K_2)$ where $\oplus$ is the bitwise XOR operation. This defines a new block cipher with n-bit blocks and $3n$-bit keys. We consider key recovery known plaintext attacks against Enc using r pairs (x_i, y_i) such that $y_i = \mathsf{Enc}_{K_1,K_2,K_3}(x_i)$ for $i = 1, \ldots, r$.

Throughout this exercise, we measure the time complexity in terms of number of C or C^{-1} operations.

Q.1 In this question, we assume that K_2 is fixed and equal to 0.

Q.1a Show that the equation $y_i = \mathsf{Enc}_{K_1,K_2,K_3}(x_i)$ can be written in the form $f_i(K_1) = g_i(K_3)$ for some functions f_i and g_i.

Q.1b Using the previous question, describe an attack method with time complexity of order of magnitude 2^n. (Justify the complexity.)

Q.1c Analyze the probability of success (the probability that it produces the correct solution and only the correct one). Propose (and justify) a minimal value for r to produce a good result.

Q.2 We now assume that K_2 is part of the secret with n bits of entropy.

Q.2a Show that the attack of the previous question can be directly adapted to obtain an attack of complexity 2^{2n}.

Q.2b Show that two equations $y_i = \mathsf{Enc}_{K_1,K_2,K_3}(x_i)$ and $y_j = \mathsf{Enc}_{K_1,K_2,K_3}(x_j)$ imply an equation which can be written in the form $f_{i,j}(K_1) = g_{i,j}(K_3)$ for some functions $f_{i,j}$ and $g_{i,j}$.

Q.2c Deduce an attack method of complexity 2^n and make the analysis like in Q.1c.

2 The Hill Cipher

Let d be an integer. We define the Hill cipher with security parameter d as follows. The message space is $\mathbf{Z}_{26}^d$. Messages are strings of d alphabetical characters encoded into $\mathbf{Z}_{26}$. The key space is the set of invertible $d \times d$ matrices over $\mathbf{Z}_{26}$. Given a key K and a message X, the encryption of X under K is $\mathsf{Enc}_K(X) = K \times X$ with operations modulo 26.

Q.1 Explain how the decryption works.

Q.2 Propose a chosen plaintext key recovery attack with complexity $\mathcal{O}(d^2)$ using d chosen plaintexts. (Justify the complexity.)
HINT: assume that read/write of a $\mathbf{Z}_{26}$ element costs $\mathcal{O}(1)$ complexity.

Q.3 Given d known plaintext/ciphertext pairs (X_i, Y_i) for $i = 1, \ldots, d$, propose a key recovery attack of complexity $\mathcal{O}(d^4)$ when $d \to +\infty$ and prove the complexity.
WARNING: d^4 is lower than d^7!
HINT: assume that the X_i vectors are linearly independent!

3 Attribute-Based Encryption

We use an *attribute-based* encryption scheme. It allows to encrypt a message respective to a set of attributes att' so that only people having privileges for at least d of these attributes can decrypt the ciphertext. People receive a secret sk corresponding to the list of attributes att that they have. Decryption works only when $\#(\mathsf{att} \cap \mathsf{att}') \geq d$. For instance, an attribute age could represent people over 25, an attribute $\mathsf{licence}$ could represent people owning a driving licence. To rent a car, customers should get an ignition key M which is encrypted for people being over 25 and with a driving licence, so with $\mathsf{att}' = \{\mathsf{age}, \mathsf{licence}\}$. Only people with att including these two privileges should be able to decrypt it and take a car. So, we would set $d = 2$. To use this scheme, an authority generates the master secret msk and the master public key mpk using Setup. Then, it gives attributes att to users and gives them a secret key sk to allow them to decrypt some ciphertexts. Finally, an encryption function using mpk and a set of attributes att' can encrypt messages.

We consider (multiplicative) groups G_1 and G_2 of prime order p and a bilinear map

$$e : G_1 \times G_1 \to G_2$$

We recall that it means that we have

$$e(u^a v^b, w) = e(u, w)^a e(v, w)^b \quad \text{and} \quad e(u, v^a w^b) = e(u, v)^a e(u, w)^b$$

for all $u, v, w \in G_1$ and $a, b \in \mathbf{Z}$. We let g be a generator of G_1. We assume that $e(g, g)$ is a generator of G_2. We consider the following algorithms.

$\mathsf{Setup}(d, n) \to (\mathsf{msk}, \mathsf{mpk})$

pick $t_1, \ldots, t_n \in \mathbf{Z}_p^*$ and $y \in \mathbf{Z}_p$ at random
set $T_i = g^{t_i}$, $i = 1, \ldots, n$ and $Y = e(g, g)^y$
set $\mathsf{mpk} = (d, T_1, \ldots, T_n, Y)$ and $\mathsf{msk} = (t_1, \ldots, t_n, y)$

$\mathsf{Gen}(\mathsf{msk}, \mathsf{att}) \to \mathsf{sk}$ $\quad \{\mathsf{msk} = (t_1, \ldots, t_n, y)$, $\mathsf{att} \subseteq \{1, \ldots, n\}$ non empty$\}$

pick some random polynomial $q \in \mathbf{Z}_p[x]$ of degree at most $d - 1$ such that $q(0) = y$ in $\mathbf{Z}_p$
set $D_i = g^{\frac{q(i)}{t_i}}$ for $i \in \mathsf{att}$
set $\mathsf{sk} = (D_i)_{i \in \mathsf{att}}$ $\{$the list of all D_i for $i \in \mathsf{att}\}$

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{att}', M) \to \mathsf{ct}$ $\quad \{\mathsf{mpk} = (d, T_1, \ldots, T_n, Y)$, $\mathsf{att}' \subseteq \{1, \ldots, n\}$ non empty, $M \in G_2\}$

pick $s \in \mathbf{Z}_p$ at random
set $E' = MY^s$ and $E_i = T_i^s$ for $i \in \mathsf{att}'$
set $\mathsf{ct} = (E', (E_i)_{i \in \mathsf{att}'})$ $\{E'$ and the list of all E_i for $i \in \mathsf{att}'\}$

Q.1 Let $i \neq j$ be two attributes. Show that there exist some $\lambda_{i,j}, \mu_{i,j} \in \mathbf{Z}_p$ such that

$$\forall a, b \in \mathbf{Z}_p \qquad \lambda_{i,j}(ai + b) + \mu_{i,j}(aj + b) = b \pmod{p}$$

Q.2 In this question, we assume that $d = 2$.
Specify a decryption algorithm $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, \mathsf{ct}) \to M'$ such that for all M, att, $i, j \in \mathsf{att}$ such that $i \neq j$, when we run

1: $\mathsf{Setup}(d, n) \to (\mathsf{msk}, \mathsf{mpk})$
2: $\mathsf{Gen}(\mathsf{msk}, \mathsf{att}) \to \mathsf{sk}$
3: $\mathsf{Enc}(\mathsf{mpk}, \{i, j\}, M) \to \mathsf{ct}$
4: $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, \mathsf{ct}) \to M'$

then we always have $M' = M$.

Q.3 More generally, let $I = \{i_1, \ldots, i_d\} \subseteq \{1, \ldots, n\}$ be a subset of size d. Show that there exists a function $\lambda_I : I \to \mathbf{Z}_p$ such that

$$\forall q \in \mathbf{Z}_p[x] \qquad \mathsf{deg}(q) \leq d - 1 \Longrightarrow \lambda_I(i_1)q(i_1) + \cdots + \lambda_I(i_d)q(i_d) = q(0) \pmod{p}$$

(q is a polynomial of degree up to $d - 1$).

Q.4 Specify a decryption algorithm $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, \mathsf{ct}) \rightarrow M'$ such that for all d, n, M, att, att' such that $\#(\mathsf{att} \cap \mathsf{att}') \geq d$, when we run

1: $\mathsf{Setup}(d, n) \rightarrow (\mathsf{msk}, \mathsf{mpk})$
2: $\mathsf{Gen}(\mathsf{msk}, \mathsf{att}) \rightarrow \mathsf{sk}$
3: $\mathsf{Enc}(\mathsf{mpk}, \mathsf{att}', M) \rightarrow \mathsf{ct}$
4: $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}, \mathsf{ct}) \rightarrow M'$

then we always have $M' = M$.