Cryptography and Security — Midterm Exam

Serge Vaudenay

27.11.2019

- 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 **not** 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 GF(256) Computations

AES used $\mathsf{GF}(2^8)$ represented by polynomials reduced modulo $x^8 + x^4 + x^3 + x + 1$ in $\mathbf{Z}_2[x]$. The InvMixColumns step of the AES decryption algorithm multiplies

$$M^{-1} = \begin{pmatrix} \texttt{0x0e} & \texttt{0x0b} & \texttt{0x0d} & \texttt{0x09} \\ \texttt{0x09} & \texttt{0x0e} & \texttt{0x0b} & \texttt{0x0d} \\ \texttt{0x0d} & \texttt{0x09} & \texttt{0x0e} & \texttt{0x0b} \\ \texttt{0x0b} & \texttt{0x0d} & \texttt{0x09} & \texttt{0x0e} \end{pmatrix}$$

by a 4-dimensional vector with coordinates in $\mathsf{GF}(2^8)$.

Q.1 What are the polynomials represented by the bytes `0x0e`, `0x0b`, `0x0d`, and `0x09`?

Q.2 Multiply the vector (`0x0e`, `0x0b`, `0x0d`, `0x09`) by the $\mathsf{GF}(2^8)$ element `0x02`. (Response must be hexadecimal.)

Q.3 Apply InvMixColumns on the column $(\texttt{0x01}, \texttt{0x02}, \texttt{0x10}, \texttt{0x40})^t$. (Response must be hexadecimal.)

2 DH in an RSA Group

A *strong* prime is an odd prime number p such that $\frac{p-1}{2}$ is also a prime number. A *strong* RSA modulus is a number $n = pq$ which is the product of two different strong primes p and q. In this exercise, we consider such a strong RSA modulus and we denote $p = 2p' + 1$, $q = 2q' + 1$, and $n' = p'q'$.

Q.1 Prove that there exists an element $g \in \mathbf{Z}_n^*$ of order n'.

Q.2 How to check group membership in the subgroup $\langle g \rangle$ of $\mathbf{Z}_n^*$?

Q.3 If n and n' are known, show that we can easily compute p and q.

Q.4 We consider a Diffie-Hellman protocol in the subgroup $\langle g \rangle$ of Z_n^*. Prove that if the factorization of n must be kept secret, there is a big problem to implement the protocol.

Q.5 Prove that the subgroup of $\mathbf{Z}_n^*$ of all x such that $(x/n) = +1$ is cyclic and of order $2n'$.

Q.6 Propose a meaningful Diffie-Hellman protocol in a cyclic subgroup of $\mathbf{Z}_n^*$ which keeps the factorization of n secret. (Carefuly check all what we need to add in the regular Diffie-Hellman protocol for security reasons.)

3 Attribute-Based Encryption

Let G_1 and G_2 be two groups with multiplicative notations and let $e : G_1 \times G_1 \to G_2$ be a non-degenerate bilinear map. We assume that G_1 is cyclic, of prime order p, and generated by some element g. We consider two parameters n and d with $d \leq n$. The tuple $\mathsf{pp} = (G_1, G_2, p, g, n, d)$ is a vector of public parameters. We consider the following algorithms:

$\mathsf{Genmaster}(\mathsf{pp})$:
- parse $\mathsf{pp} = (G_1, G_2, p, g, n, d)$
- pick $t_1, \ldots, t_n, y \in \mathbf{Z}_p$ at random
- $T_1 \leftarrow g^{t_1}$, ..., $T_n \leftarrow g^{t_n}$, $Y \leftarrow e(g,g)^y = e(g^y, g)$
- $\mathsf{pk} \leftarrow (T_1, \ldots, T_n, Y)$
- $\mathsf{mk} \leftarrow (t_1, \ldots, t_n, y)$
- **return** $(\mathsf{pk}, \mathsf{mk})$

$\mathsf{Gen}(\mathsf{pp}, \mathsf{mk}, A)$: $\triangleright$ $A \subseteq \{1, \ldots, n\}$
- parse $\mathsf{pp} = (G_1, G_2, p, g, n, d)$
- pick a random polynomial $q(x) \in \mathbf{Z}_p[x]$ of degree $d-1$ such that $q(0) = y$
- for each $i \in A$, $D_i \leftarrow g^{\frac{q(i)}{t_i}}$
- $\mathsf{sk} \leftarrow (D_i)_{i \in A}$
- **return** sk

$\mathsf{Enc}(\mathsf{pp}, \mathsf{pk}, m, B)$: $\triangleright$ $m \in G_2$, $B \subseteq \{1, \ldots, n\}$
- parse $\mathsf{pp} = (G_1, G_2, p, g, n, d)$
- pick $s \in \mathbf{Z}_p$ at random
- $E \leftarrow mY^s$
- for each $i \in B$, $E_i \leftarrow T_i^s$
- $\mathsf{ct} \leftarrow (B, E, (E_i)_{i \in B})$
- **return** ct

In our system, Genmaster returns a public key pk (given to anyone with pp) and a master secret mk for a trusted dealer. Each user U has a set of attributes A_U and the trusted dealer gives him a secret sk_U which is generated by $\mathsf{Gen}(\mathsf{pp}, \mathsf{mk}, A_U)$. Anyone can encrypt a message m with some set of attributes B.

Q.1 Express ct in terms of pp, mk, m, and s.

Q.2 Show how to decrypt ct given pp and pk by assuming that the discrete logarithm problem is easy. (Assume B non empty.)

Q.3 Show that if $A \cap B$ has cardinality at least d, then we can easily decrypt ct given pp and sk. (I.e., we do not need to compute a discrete logarithm.)