Cryptography and Security — Midterm Exam

Solution

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

The exam grade follows a linear scale in which each question has the same weight.

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`?

The hexadecimal representation is a shorthand for the binary representation which lists the coefficients of the polynomial. The most significant bit is the coefficient of highest degree.

$$\begin{aligned} \texttt{0x0e} &= x^3 + x^2 + x \\ \texttt{0x0b} &= x^3 + x + 1 \\ \texttt{0x0d} &= x^3 + x^2 + 1 \\ \texttt{0x09} &= x^3 + 1 \end{aligned}$$

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

As $\texttt{0x02} = x$*, we have*

$$\mathsf{0x02} \times (\texttt{0x0e}, \texttt{0x0b}, \texttt{0x0d}, \texttt{0x09}) = (\texttt{0x1c}, \texttt{0x16}, \texttt{0x1a}, \texttt{0x12})$$

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

$$M^{-1} = \begin{pmatrix} \texttt{0x0e} & \texttt{0x0b} & \texttt{0x0d} & \texttt{0x09} \\ \texttt{0x09} & \texttt{0x0e} & \texttt{0x0b} & \texttt{0x0d} \\ \texttt{0x0d} & \texttt{0x09} & \texttt{0x0e} & \texttt{0x0b} \\ \texttt{0x0b} & \texttt{0x0d} & \texttt{0x09} & \texttt{0x0e} \end{pmatrix} \times \begin{pmatrix} \texttt{0x01} \\ \texttt{0x02} \\ \texttt{0x10} \\ \texttt{0x40} \end{pmatrix} = \begin{pmatrix} \texttt{0xbe} \\ \texttt{0xc8} \\ \texttt{0x09} \\ \texttt{0x2c} \end{pmatrix}$$

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'.

Thanks to the Chinese Remainder Theorem, we know that $g^x \bmod n = 1$ is equivalent to $g^x \bmod p = 1$ and $g^x \bmod q = 1$ (this is due to $n = pq$ and p and q being coprime). We know that $\mathbf{Z}_p^*$ is cyclic of order $p-1$ (this is due to p being prime). Hence, there exists an element $h \in \mathbf{Z}_p^*$ of order $p - 1 = 2p'$. The element $g_p = h^2 \bmod p$ is an element of $\mathbf{Z}_p^*$ of order p'. Similarly, there exists an element g_q of $\mathbf{Z}_q^*$ of order q'. We let $g \in \mathbf{Z}_n$ be such that $g \bmod p = g_p$ and $g \bmod q = g_q$, thanks to the Chinese Remainder Theorem. We have that $g^x \bmod n = 1$ is equivalent to x is a multiple of p' and q'. Since p' and q' are coprime, this is equivalent to x being a multiple of $n' = p'q'$. Hence, $g^x \bmod n = 1$ is equivalent to x is a multiple of n'. We deduce that g has order n' in $\mathbf{Z}_n^*$.

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

We have seen in the course that $x \in \langle g_p \rangle$, the subgroup of $\mathbf{Z}_p^*$ is equivalent to $x^{p'} \bmod p = 1$. We show below that $x \in \langle g \rangle$ is equivalent to $x^{n'} \bmod n = 1$.
The $x \in \langle g \rangle \implies x^{n'} \bmod n = 1$ direction is trivial: since g has order n', any power of g has an n'th power equal to 1.
We now prove $x^{n'} \bmod n = 1 \implies x \in \langle g \rangle$. We assume that $x^{n'} \bmod n = 1$. This implies that $x^{n'} \bmod p = 1$. Let $d = \frac{1}{q'} \bmod 2p'$ (we know that q' and $2p'$ are coprime). We know that $y^d \bmod p$ is the unique q'th root of y modulo p. Hence,

$$1 \equiv (x^{n'})^d \equiv x^{p'} \pmod{p}$$

We deduce that x belongs to the subgroup of $\mathbf{Z}_p^*$ generated by g. Let $x \equiv g^i \pmod{p}$. Similarly, we show there exist j such that $x \equiv g^j \pmod{q}$. We let k be such that $k \bmod p' = i$ and $k \bmod q' = j$ (we use the Chinese Remainder Theorem for the two coprime p' and q'). We have $x \equiv g^k \pmod{p}$ and $x \equiv g^k \pmod{q}$. Hence, $x \in \langle g \rangle$.

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

We have $n = (2p' + 1)(2q' + 1) = 4p'q' + 2(p' + q') + 1$ and $n' = p'q'$. Hence, p' and q' are the two roots of $x^2 - \frac{n-4n'-1}{2}x + n' = 0$. We can compute them by solving the equation over the integers. We deduce 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.

If the factorization of n is known, there is no advantage in doing the Diffie-Hellman protocol modulo n: we can do it modulo p and modulo q separately. So, we assume there can only be an advantage when the factorization of n is secret.
The protocol would require to check subgroup membership. With the above g, the only way we know for that is to raise to the power n' but this leaks the factorization of n. We could further prove that membership to $\langle g \rangle$ is equivalent to being a quadratic residue modulo p and modulo q at the same time. But distinguishing such elements from elements with Jacobi symbol $(./n)$ equal to 1 is believed to be a hard problem. Hence, we believe that there is no meaningful way to have a Diffie-Hellman protocol in $\langle g \rangle$.

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

By CRT-combining a generator modulo p and modulo q, we obtain some h such that $h^x \bmod n = 1$ is equivalent to x being a multiple of $2p'$ and $2q'$ at the same time, hence being a multiple of $2p'q'$. Hence, h has order $2p'q' = 2n'$.
h has Legendre symbols (h/p) and (h/q) which are equal. Thus, h is such that all powers of h have Legendre symbols $(./p)$ and $(./q)$ which are equal. Hence, the Jacobi symbol $(./n)$ is equal to $+1$. The subgroup spanned by h is included in the subgroup of residues with Jacobi symbol equal to $+1$. Since the full group has order $4n'$ and that there exists elements with Jacobi symbol equal to -1, this subgroup cannot have an order larger than $2n'$ (because it must be a factor of $4n'$ and there is no larger factor except $4n'$ itself). Hence, all residues of Jacobi symbol $+1$ are generated by h. Furthermore, membership to $\langle h \rangle$ is equivalent to having a Jacobi symbol $(./n)$ equal to $+1$. We have an easy membership test.

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.)

The Diffie-Hellman protocol is defined over a cyclic group. One problem is that $\mathbf{Z}_n^*$ (which has order $4p'q'$) is not cyclic. Indeed, there are four square roots of 1 so it has three elements of order 2. Cyclic groups cannot have more than one element of order 2. We have seen that the subgroup of order $p'q'$ may require to leak p and q. Thus, we can try a subgroup of order $2p'q'$.

We design a Diffie-Hellman protocol in $\langle h \rangle$ from the previous question. We check subgroup membership by checking the Jacobi symbol.

We must avoid the subgroups of $\langle h \rangle$. The trivial subgroup $\{1\}$ is checked trivially. The subgroup of order 2 is $\{1, -1\}$. (The two other square roots of 1 are not in $\langle h \rangle$.) It is also checked trivially.

The other subgroups are rare. Indeed, if an adversary manages to find an element x of them, he can factor n as follows: we have $x^{2p'} \bmod n = 1$ or $x^{2q'} \bmod n = 1$. Let assume without loss of generality that $x^{2p'} \bmod n = 1$. We have $x^{2p'} \bmod q = 1$. Since p' is invertible modulo q', we deduce that $x^2 \bmod q = 1$. Hence, $x^2 - 1$ is a multiple of q. It cannot be a multiple of n, otherwise we would fall back to the cases $x \in \{1, -1\}$ which was eliminated. Hence, $\mathsf{gcd}(x^2 - 1, n) = q$. We can compute this using the Euclid algorithm and deduce p and q. Therefore, assuming that factoring is hard, the adversary will not be able to find an element in another subgroup.

In the case Alice and Bob know the factorization, they should not help the adversary for that. Hence, they generate a secret key in $\mathbf{Z}_{2n'}^*$:

- Participants pick a secret $x \in \mathbf{Z}_{2n'}^*$ and send $y = g^x \bmod n$.
- Upon receiving z from counterpart, participants check that $(z/n) = +1$ and that $z \bmod n \not\in \{+1, n-1\}$.
- The shared key is $\mathsf{KDF}(z^x \bmod n)$.

In the case Alice and Bob ignore the factorization, they have a little problem to sample their secret. For that they can generate some x of "double size", i.e. in $\{2, \ldots, n^2 - 1\}$.

- Participants pick a secret $x \in \{2, \ldots, n^2 - 1\}$ and compute $y = g^x \bmod n$.
- If $y = 1$ or $y = n - 1$, try again.
- Upon receiving z from counterpart, participants check that $(z/n) = +1$ and that $z \bmod n \not\in \{+1, n-1\}$.
- The shared key is $\mathsf{KDF}(z^x \bmod n)$.

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:

```
Genmaster(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 $(\mathsf{pk}, \mathsf{mk})$

Gen(pp, mk, $A$):                                   ▷ $A \subseteq \{1, \ldots, n\}$
  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

Enc(pp, pk, $m$, $B$):                              ▷ $m \in G_2$, $B \subseteq \{1, \ldots, n\}$
  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.

We have $E = mY^s = me(g, g)^{ys}$ and $E_i = T_i^s = g^{t_i s}$ for each $i \in A$.

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

Given one $i \in B$, the discrete logarithm of $T_i = g^{t_i}$ gives t_i. Then, $E_i^{\frac{1}{t_i} \bmod p} = g^s$. Then, $E/Y^s = m$.

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.)

Let $C \subseteq A \cap B$ of cardinality exactly d. Let $C = \{i_1, \ldots, i_d\}$. There exists some coefficients $\lambda_1, \ldots, \lambda_d$ (the Lagrange coefficients) such that $\sum_{j=1}^{d} \lambda_j q(i_j) = q(0)$ for any polynomial q of degree $d-1$. Actually, the following formula gives those coefficients:

$$\lambda_j = \frac{\prod_{k \in \{1,\ldots,j-1,j+1,\ldots,d\}} i_k}{\prod_{k \in \{1,\ldots,j-1,j+1,\ldots,d\}} (i_k - i_j)}$$

Hence,

$$\prod_{j=1}^{d} e(D_{i_j}, E_{i_j})^{\lambda_j} = \prod_{j=1}^{d} e(g,g)^{s\lambda_j q(i_j)} = e(g,g)^{sq(0)} = e(g,g)^{sy} = Y^s$$

Therefore, we can divide E by this to obtain m.