Cryptography and Security — Midterm Exam

Serge Vaudenay

24.11.2011

- duration: 1h45
- no documents is allowed
- a pocket calculator is allowed
- communication devices are not allowed
- exam proctors will not answer any technical question during the exam
- answers to every exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 A Weird Mode of Operation

In this exercise, we assume that we have a block cipher C and we use it in the following mode of operation: to encrypt a sequence of blocks $x_1, \ldots, x_n$, we initialize a counter t to some IV value, then we compute

$$y_i = t_i \oplus C_K(x_i)$$

for every i where K is the encryption key and $t_i = \mathsf{IV} + i$. The ciphertext is

$$\mathsf{IV}, y_1, \ldots, y_n$$

Namely, IV is sent in clear.

Q.1 Is this mode of operation equivalent to something that you already know? Say why?
Q.2 Does the IV need to be unique?
Q.3 What kind of security problem does this mode of operation suffer from?

2 RSA Modulo 1 000 001

Given $a_1, a_2, \ldots, a_n \in \{0, 1, \ldots, 9\}$, we denote by $\overline{a_1 a_2 \cdots a_n}$ the decimal number equal to $10(10(\cdots 10a_1 + a_2 \cdots) + a_{n-1}) + a_n$.

Q.1 Consider a decimal number $\overline{abc\,def}$. Show that

$$\overline{abc\,def} \equiv \overline{ab} - \overline{cd} + \overline{ef} \pmod{\mathbf{101}}$$

As an application, compute 336 634 mod 101 and 663 368 mod 101.
Q.2 Compute the inverse of $x = 1\,000$ modulo $p = 101$.
Q.3 Consider a decimal number $\overline{abc\,def}$. Show that

$$\overline{abc\,def} \equiv \overline{ab00} - \overline{ab} + \overline{cdef} \pmod{\mathbf{9\,901}}$$

As an application, compute 336 634 mod 9 901 and 663 368 mod 9 901.
Q.4 Compute $x^{199} \bmod q$ for $x = 1\,000$ and $q = 9\,901$.

Q.5 Given a and b, show that $x = 336\,634a + 663\,368b$ is such that $x \bmod 101 = a$ and $x \bmod 9\,901 = b$.

Q.6 Given $p = 101$ and $q = 9\,901$, we let $N = pq$. Compute $\varphi(N)$ and factor it into a product of prime numbers.

Q.7 Let e be an integer. Show that e is a valid RSA exponent for modulus N if and only if there is no prime factor of $\varphi(N)$ dividing e.

Q.8 Show that $e = 199$ is a valid RSA exponent for modulus N and compute the encryption of $x = 1\,000$ for this public key.

3 AES Galois Field and AES Decryption

We briefly recall the AES block cipher here. It encrypts a block specified as a 4×4 matrix of bytes s and using a sequence $W_0, \ldots, W_n$ of matrices which are derived from a secret key. For convenience the row and columns indices range from 0 to 3. For instance, $s_{1,3}$ means the term of s in the second row and last column. The main AES encryption function is defined by the following pseudocode:

AESencryption(s, W)
AddRoundKey(s, W_0)
for $r = 1$ to $n - 1$ **do**
  SubBytes(s)
  ShiftRows(s)
  MixColumns(s)
  AddRoundKey(s, W_r)
end for
SubBytes(s)
ShiftRows(s)
AddRoundKey(s, W_n)

AddRoundKey(s, W_r) is replacing s by $s \oplus W_r$, the component-wise XOR of matrices s and W_r. **SubBytes**(s) is replacing s by a new matrix in which the term at position i, j is $S(s_{i,j})$, where S is a fixed permutation of the set of all byte values. **ShiftRows**(s) is replacing s by a new matrix in which the term at position i, j is $s_{i,i+j \bmod 4}$. **MixColumns**(s) is replacing s by a new matrix in which the column at position j is $M \times s_{\cdot,j}$, where $s_{\cdot,j}$ denotes the column at position j of s and M is a fixed matrix defined by

$$M = \begin{pmatrix} \texttt{0x02} & \texttt{0x03} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x02} & \texttt{0x03} & \texttt{0x01} \\ \texttt{0x01} & \texttt{0x01} & \texttt{0x02} & \texttt{0x03} \\ \texttt{0x03} & \texttt{0x01} & \texttt{0x01} & \texttt{0x02} \end{pmatrix}$$

The matrix product inherits from the algebraic structure $\mathsf{GF}(256)$ on the set of all byte values. Namely, each byte represents a polynomial on variable x of degree at most 7 and coefficients in $\mathbf{Z}_2$. Polynomials are added and multiplied modulo 2 and modulo $P(x) = x^8+x^4+x^3+x+1$. The correspondence between bytes and polynomial works as follows: each byte a is a sequence of 8 bits $a_7, \ldots, a_0$ which is represented in hexadecimal `0x`uv where u and v are two hexadecimal digits (i.e. between `0` and `f`), u encodes $a_7a_6a_5a_4$, and v encodes $a_3a_2a_1a_0$ by the following encoding rule:

0000→0	0100→4	1000→8	1100→c
0001→1	0101→5	1001→9	1101→d
0010→2	0110→6	1010→a	1110→e
0011→3	0111→7	1011→b	1111→f

Q.1 Provide a pseudocode for **AESdecryption**(s, W), for AES decryption.
Q.2 Which polynomial does `0x2b` represent?
Q.3 Compute `0x53` + `0xb8`.
Q.4 Compute `0x21` × `0x25`.
Q.5 Compute the inverse of `0x02`.
Hint: look at $P(x)$.
Q.6 Show that M^{-1} is of form

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

where all missing terms are in the set $\{\texttt{0x09}, \texttt{0x0b}, \texttt{0x0d}, \texttt{0x0e}\}$.