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 $t_i = IV + i$. The ciphertext is $IV, y_1, \ldots, y_n$.

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 $\overline{a_1a_2\cdots a_n}$ the decimal number equal to $10(10(\cdots 10a_1 + a_2 \cdots) + a_{n-1}) + a_n$.

Q.1 Consider a decimal number $\overline{abcdef}$. Show that

$$\overline{abcdef} \equiv \overline{ab} - \overline{cd} + \overline{ef} \pmod{101}$$

As an application, compute $336\,634 \mod 101$ and $663\,368 \mod 101$.

Q.2 Compute the inverse of $x = 1000$ modulo $p = 101$.

Q.3 Consider a decimal number $\overline{abcdef}$. Show that

$$\overline{abcdef} \equiv \overline{ab00} - \overline{a0} + \overline{cdef} \pmod{9 \, 901}$$

As an application, compute $336\,634 \mod 9\,901$ and $663\,368 \mod 9\,901$.

Q.4 Compute $x^{199} \mod q$ for $x = 1000$ and $q = 9\,901$. 

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

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 \( 4 \times 4 \) 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 column 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:

\[
\text{AESencryption}(s, W) \\
\begin{align*}
1: & \quad \text{AddRoundKey}(s, W_0) \\
2: & \quad \text{for } r = 1 \text{ to } n - 1 \text{ do} \\
3: & \quad \quad \text{SubBytes}(s) \\
4: & \quad \quad \text{ShiftRows}(s) \\
5: & \quad \quad \text{MixColumns}(s) \\
6: & \quad \quad \text{AddRoundKey}(s, W_r) \\
7: & \quad \text{end for} \\
8: & \quad \text{SubBytes}(s) \\
9: & \quad \text{ShiftRows}(s) \\
10: & \quad \text{AddRoundKey}(s, W_n)
\end{align*}
\]

\( \text{AddRoundKey}(s, W_r) \) is replacing \( s \) by \( s \oplus W_r \), the component-wise XOR of matrices \( s \) and \( W_r \). \( \text{SubBytes}(s) \) 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. \( \text{ShiftRows}(s) \) is replacing \( s \) by a new matrix in which the term at position \( i, j \) is \( s_{i,i+j \mod 4} \). \( \text{MixColumns}(s) \) is replacing \( s \) by a new matrix in which the column at position \( j \) is \( M \times s_{-,j} \), where \( s_{-,j} \) denotes the column at position \( j \) of \( s \) and \( M \) is a fixed matrix defined by

\[
M = \begin{pmatrix}
0x02 & 0x03 & 0x01 & 0x01 \\
0x01 & 0x02 & 0x03 & 0x01 \\
0x01 & 0x01 & 0x02 & 0x03 \\
0x03 & 0x01 & 0x01 & 0x02
\end{pmatrix}
\]

The matrix product inherits from the algebraic structure \( \mathbb{GF}(256) \) on the set of all byte values. Namely, each byte represents a polynomial on variable \( x \) of degree at most 7 and coefficients in \( \mathbb{Z}_2 \). 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 \( 0xuv \) 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:
Q.1 Provide a pseudocode for AES decryption $(s, W)$, for AES decryption.

Q.2 Which polynomial does 0x2b represent?

Q.3 Compute $0x53 + 0xb8$.

Q.4 Compute $0x21 \times 0x25$.

Q.5 Compute the inverse of 0x02.
   
   **Hint:** look at $P(x)$.

Q.6 Show that $M^{-1}$ is of form

\[
M^{-1} = \begin{pmatrix}
0x0e & 0x0b & 0x0d & 0x09 \\
0x09 & \cdot & \cdot & \cdot \\
0x0d & \cdot & \cdot & \cdot \\
0x0b & \cdot & \cdot & \cdot 
\end{pmatrix},
\]

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

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