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 \( t_i = \text{IV} + i \). The ciphertext is

\[
\text{IV}, y_1, \ldots, y_n
\]

Namely, IV is sent in clear.

**Q.1** Is this mode of operation equivalent to something that you already know? Say why?

*It is equivalent to the ECB mode. Namely, a passive adversary can compute \( t_i \) and then \( y_i \oplus t_i \) for every \( i \). This gives the ECB encryption of \( x_1, \ldots, x_n \).*

**Q.2** Does the IV need to be unique?

*No.*

**Q.3** What kind of security problem does this mode of operation suffer from?

*Like the ECB mode, if the entropy of a block \( x_i \) is low, then \( y_i \oplus t_i \) repeats. For instance, \( x_i = x_j \) is equivalent to \( y_i \oplus t_i = y_j \oplus t_j \) which can be observed with values which are sent over the insecure channel.*
2 RSA Modulo 1 000 001

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

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

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

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

We have

$$\overline{abcdef} = 10(10(10(10a + b) + c) + d) + e) + f$$

$$= 100^2(10a + b) + 100(10c + d) + (10e + f)$$

Since $100 \equiv -1 \pmod{101}$, this writes

$$\overline{abcdef} \equiv (10a + b) - (10c + d) + (10e + f) \pmod{101}$$

which is what we had to prove. So,

$$336 634 \equiv 33 - 66 + 34 = 1 \pmod{101}$$

and

$$663 368 \equiv 66 - 33 + 68 = 101 \equiv 0 \pmod{101}$$

which yields $336 634 \mod 101 = 1$ and $663 368 \mod 101 = 0$.

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

A general method consists of applying the extended Euclid algorithm. We have

$$x_1 = (1000, 1, 0) \quad x_2 = (101, 0, 1)$$
$$x_3 = (101, 0, 1) \quad x_3 = (91, 1, -9) \quad x_3 = x_1 - 9x_2$$
$$x_4 = (91, 1, -9) \quad x_4 = (10, -1, 10) \quad x_4 = x_2 - x_3$$
$$x_5 = (10, -1, 10) \quad x_5 = (1, 10, -99) \quad x_5 = x_3 - 9x_4$$
$$x_6 = (1, 10, -99) \quad x_6 = (0, -101, 1000) \quad x_6 = x_4 - 10x_5$$

so $1 = 1000 \times 10 - 101 \times 99$. Therefore, $x^{-1} \mod p = 10$.

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

$$\overline{abcdef} \equiv \overline{ab00} - \overline{ab} + \overline{cd} + \overline{ef} \pmod{9901}$$

As an application, compute $336 634 \mod 9901$ and $663 368 \mod 9901$. 

Just like before, we have
\[
abc\text{def} = 10(10(10a+b)+c)+d+e+f = 10^4(10a+b+cdef)
\]
Since \(10^4 \equiv 100 - 1 \pmod{9901}\), this writes
\[
abc\text{def} \equiv 100(10a+b) - (10a+b) + cdef \pmod{101}
\]
which is what we had to prove. So,
\[
336634 \equiv 3300 - 33 + 6634 = 9901 \equiv 0 \pmod{9901}
\]
and
\[
663368 \equiv 6600 - 66 + 3368 = 9902 \equiv 1 \pmod{9901}
\]
which yields \(336634 \pmod{101} = 0\) and \(663368 \pmod{101} = 1\).

**Q.4** Compute \(x^{199} \pmod{q}\) for \(x = 1000\) and \(q = 9901\).

Then, \(x^{199} \equiv x^4 \times (x^4)^{49} \pmod{q}\). We have
\[
x^2 = 1000^2 = 1000000 \equiv 10000 - 100 + 000 = 9900 \equiv -1 \pmod{q}
\]
so \(x^4 \equiv 1 \pmod{q}\) and \(x^3 \equiv -x \pmod{q} = 8901\). Thus, \(b = 8901\).

Applying the square-and-multiply algorithm would have led to \(x^4 \pmod{q} = 1\) as well.

**Q.5** Given \(a\) and \(b\), show that \(x = 336634a + 663368b\) is such that \(x \pmod{101} = a\) and \(x \pmod{9901} = b\).

We have \(336634 \pmod{101} = 1\) and \(663368 \pmod{101} = 0\) so, by linearity, we have \(x \equiv a \pmod{101}\). We have \(336634 \pmod{9901} = 0\) and \(663368 \pmod{9901} = 1\) so, by linearity, we have \(x \equiv b \pmod{9901}\). This expression for \(x\) is actually the inverse formula for the Chinese remainder theorem using moduli 101 and 9901 (note that they are coprime).

**Q.6** Given \(p = 101\) and \(q = 9901\), we let \(N = pq\). Compute \(\varphi(N)\) and factor it into a product of prime numbers.

Since \(p\) and \(q\) are prime, we have
\[
\varphi(N) = (p-1)(q-1) = 100 \times 9900 = 990000 = 10^4 \times 9 \times 11 = 2^4 \times 3^2 \times 5^4 \times 11
\]

**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 \(e\).

\(e\) is a valid RSA exponent if and only if \(\gcd(e, \varphi(N)) = 1\) which is if and only if none of the prime factors of \(\varphi(N)\) divide \(e\). Since the list of prime factors of \(\varphi(N)\) is \(\{2,3,5,11\}\), we obtain the result.
Q.8 Show that \( e = 199 \) is a valid RSA exponent for modulus \( N \) and compute the encryption of \( x = 1000 \) for this public key.

\[ 199 \text{ has no prime factor in } \{2, 3, 5, 11\} \text{ so it is a valid exponent. To compute } x^e \mod N, \text{ we use the Chinese remainder theorem. We compute } a = x^e \mod p \text{ and } b = x^e \mod q. \]

\[ \text{We have } a = x^{199} \mod 101 = x^{199 \mod 100} \mod 101 = x^{-1} \mod 101 = 10 \text{ due to Q.2.} \]

\[ \text{Similarly, we have } b = x^{199} \mod 9901 = 8901 \text{ due to Q.4. Finally,} \]

\[ x^e \mod N = (336\,634 \times 10 + 663\,368 \times 8901) \mod N = 5\,908\,004\,908 \mod N = 999\,001 \]

\[ \text{So, the encryption of } x \text{ is } 999\,001. \]
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 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:

$$\text{AES encryption}(s, W)$$

1. AddRoundKey($s, W_0$)
2. for $r = 1$ to $n - 1$ do
3. SubBytes($s$)
4. ShiftRows($s$)
5. MixColumns($s$)
6. AddRoundKey($s, W_r$)
7. end for
8. SubBytes($s$)
9. ShiftRows($s$)
10. AddRoundKey($s, W_n$)

$\text{AddRoundKey}(s, W_r)$ 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 $M \cdot s_{.j}$, 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 $\text{GF}(256)$ 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 $0uv$ 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:

<table>
<thead>
<tr>
<th>Bit Sequence</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>00000000</td>
</tr>
<tr>
<td>0001</td>
<td>00010000</td>
</tr>
<tr>
<td>0010</td>
<td>00101000</td>
</tr>
<tr>
<td>0011</td>
<td>00110000</td>
</tr>
<tr>
<td>0100</td>
<td>01000000</td>
</tr>
<tr>
<td>0101</td>
<td>01010000</td>
</tr>
<tr>
<td>0110</td>
<td>01100000</td>
</tr>
<tr>
<td>0111</td>
<td>01110000</td>
</tr>
<tr>
<td>1000</td>
<td>10000000</td>
</tr>
<tr>
<td>1001</td>
<td>10010000</td>
</tr>
<tr>
<td>1010</td>
<td>10100000</td>
</tr>
<tr>
<td>1011</td>
<td>10110000</td>
</tr>
<tr>
<td>1100</td>
<td>11000000</td>
</tr>
<tr>
<td>1101</td>
<td>11010000</td>
</tr>
<tr>
<td>1110</td>
<td>11100000</td>
</tr>
<tr>
<td>1111</td>
<td>11110000</td>
</tr>
</tbody>
</table>

Q.1 Provide a pseudocode for $\text{AES decryption}(s, W)$, for AES decryption.
We remark that \textbf{AddRoundKey} is self-inverse. We further remark that \textbf{SubBytes} and \textbf{ShiftRows} commute.

\textbf{AESdecryption}(s; W)
1: \textbf{AddRoundKey}(s, W_n)
2: \textit{for} \( r = n - 1 \) \textit{down to} 1 \textit{do}
3: \textbf{InvSubBytes}(s)
4: \textbf{InvShiftRows}(s)
5: \textbf{AddRoundKey}(s, W_r)
6: \textbf{InvMixColumns}(s)
7: \textit{end for}
8: \textbf{InvSubBytes}(s)
9: \textbf{InvShiftRows}(s)
10: \textbf{AddRoundKey}(s, W_0)

\textbf{InvSubBytes}(s) is replacing \textit{s} by a new matrix in which the term at position \( i, j \) is \( S^{-1}(s_{i,j}) \). \textbf{InvShiftRows}(s) is replacing \textit{s} by a new matrix in which the term at position \( i, j \) is \( s_{i, -i+j \mod 4} \). \textbf{InvMixColumns}(s) is replacing \textit{s} by a new matrix in which the column at position \( j \) is \( M^{-1} \times s_{j} \).

Q.2 Which polynomial does \textit{0x2b} represent?

\textit{2 encodes} 0010 and \textit{b} encodes 1011, so \textit{0x2b} encodes the bitstring 0010 1011 which represents \( x^5 + x^3 + x + 1 \).

Q.3 Compute \textit{0x53 + 0xb8}.

\textit{Addition is a simple XOR}. \textit{0x53 encodes} 0101 0011 and \textit{0xb8 encodes} 1011 1000. \textit{The XOR is} 1110 1011 which is encoded by \textit{0xeb}. So, \textit{0x53 + 0xb8 = 0xeb}.

Q.4 Compute \textit{0x21 \times 0x25}.

\textit{0x21 represents the polynomial} \( x^5 + 1 \). \textit{0x25 represents the polynomial} \( x^9 + x^2 + 1 \). \textit{We have}

\[ (x^5 + 1) \times (x^5 + x^2 + 1) = x^{10} + x^7 + 2x^5 + x^2 + 1 \equiv x^{10} + x^7 + x^2 + 1 \]

\textit{Since} \( x^8 \equiv x^4 + x^3 + x + 1 \) \textit{we have} \( x^9 \equiv x^5 + x^4 + x^2 + x \) \textit{and} \( x^{10} \equiv x^6 + x^5 + x^3 + x^2 \).

\textit{So,}

\[ (x^5+1)\times(x^5+x^2+1) \equiv x^{10}+x^7+x^2+1 \equiv x^7+x^6+x^5+x^3+2x^2+1 \equiv x^7+x^6+x^5+x^3+1 \]

\textit{Now,} \( x^7 + x^6 + x^5 + x^3 + 1 \) \textit{is represented by} \textit{0xe9}. \textit{So,} \( 0x21 \times 0x25 = 0xe9 \).

Q.5 Compute the inverse of \textit{0x02}.

\textbf{Hint:} look at \( P(x) \).

\textit{Since} \( x^8 + x^4 + x^3 + x + 1 \equiv 0 \), \textit{by multiplying by} \( x^{-1} \) \textit{we obtain} \( x^7 + x^3 + x^2 + 1 + x^{-1} \equiv 0 \), \textit{so} \( x^{-1} = x^7 + x^3 + x^2 + 1 \). \textit{Changing this into hexadecimal bytes, this gives}

\[ 0x02^{-1} = 0x8d \]
Q.6 Show that $M^{-1}$ is of form

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

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

\[
\begin{pmatrix}
0x02 & 0x03 & 0x01 & 0x01 \\
0x01 & 0x02 & 0x03 & 0x01 \\
0x01 & 0x01 & 0x02 & 0x03 \\
0x03 & 0x01 & 0x01 & 0x02 
\end{pmatrix}
\times
\begin{pmatrix}
0x0e \\
0x09 \\
0x0d \\
0x0b
\end{pmatrix}
= M \times \begin{pmatrix}
0x0e \\
0x09 \\
0x0d \\
0x0b
\end{pmatrix}
\]

By writing this with polynomials, this gives

\[
M \times \begin{pmatrix}
0x0e \\
0x09 \\
0x0d \\
0x0b
\end{pmatrix}
= \begin{pmatrix}
x & x+1 & 1 & 1 \\
1 & x & x+1 & 1 \\
x+1 & 1 & 1 & x 
\end{pmatrix}
\times
\begin{pmatrix}
x^3 + x^2 + x \\
x^3 + 1 \\
x^3 + x^2 + 1 \\
x^3 + x + 1
\end{pmatrix}
= \begin{pmatrix}
1 \\
0 \\
0 \\
0
\end{pmatrix}
\]

By rotating the columns of \( M \) and the rows of the vector in the product we obtain

\[
\begin{pmatrix}
0x02 & 0x03 & 0x01 & 0x01 \\
0x01 & 0x02 & 0x03 & 0x01 \\
0x01 & 0x01 & 0x02 & 0x03 \\
0x03 & 0x01 & 0x01 & 0x02 
\end{pmatrix}
\times
\begin{pmatrix}
0x0b \\
0x0e \\
0x09 \\
0x0d
\end{pmatrix}
= \begin{pmatrix}
1 \\
0 \\
0 \\
0
\end{pmatrix}
\]

Now, by rotating the rows of the matrix and of the result, we obtain

\[
\begin{pmatrix}
0x02 & 0x03 & 0x01 & 0x01 \\
0x01 & 0x02 & 0x03 & 0x01 \\
0x01 & 0x01 & 0x02 & 0x03 \\
0x03 & 0x01 & 0x01 & 0x02 
\end{pmatrix}
\times
\begin{pmatrix}
0x0b \\
0x0e \\
0x09 \\
0x0d
\end{pmatrix}
= M \times \begin{pmatrix}
0x0b \\
0x0e \\
0x09 \\
0x0d
\end{pmatrix}
= \begin{pmatrix}
0 \\
1 \\
0 \\
0
\end{pmatrix}
\]

By redoing the same, we obtain

\[
M \times \begin{pmatrix}
0x0d \\
0x0b \\
0x0e \\
0x09
\end{pmatrix}
= \begin{pmatrix}
0 \\
1 \\
0 \\
0
\end{pmatrix}
\]

and

\[
M \times \begin{pmatrix}
0x09 \\
0x0d \\
0x0b \\
0x0e
\end{pmatrix}
= \begin{pmatrix}
0 \\
0 \\
0 \\
1
\end{pmatrix}
\]

So,

\[
M \times \begin{pmatrix}
0x0e & 0x0b & 0x0d & 0x09 \\
0x09 & 0x0e & 0x0b & 0x0d \\
0x0d & 0x09 & 0x0e & 0x0b \\
0x0b & 0x0d & 0x09 & 0x0e
\end{pmatrix}
= \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

which gives the inverse of \( M \) and proves the required properties.