1 AES-Hashing

In this exercise we consider a special hash function \( H \) defined as follows. To hash a message \( m \) with a length multiple of 256 bits, we split it into blocks of 256 bits \( m_1, \ldots, m_b \). Then, we compute the encryption of \( i \) with key \( m_i \) using AES for \( i = 1, \ldots, b \) and XOR them all together. We define

\[
H(m_1||\cdots||m_b) = \bigoplus_{i=1}^{b} \text{AES}_{m_i}(i)
\]

1. What is the length of the digest?
   Ideally, what should be the complexity of the best collision attack on \( H \)?
   Ideally, what should be the complexity of the best preimage attack on \( H \)?
2. Derive a collision attack to find two messages \( m \) and \( m' \) of length 256 bits with same digest.
   What is its complexity?
3. Derive a preimage attack to find a preimage of the digest 0 and finding a message of length 512 bits.
   What is its complexity?
4. Derive a second preimage attack finding a message of length 512 bits for any first preimage.
   What is its complexity?
5. Let \( m \) and \( m' \) be two messages of same bitlength 256b for an integer \( b \). Let \( m = m_1||\cdots||m_b \) and \( m' = m'_1||\cdots||m'_b \) be the decomposition into 256-bit blocks. We assume that \( m \) and \( m' \) are selected such that \( m_i \neq m'_i \) for \( i = 1, \ldots, b \). Let \( u_i = \text{AES}_{m_i}(i) \oplus \text{AES}_{m'_i}(i) \).
   How large should \( b \) be so that with high probability, for any \( y \) there exists a subset \( I \) of \( \{1, \ldots, b\} \) such that \( y = \bigoplus_{i \in I} u_i \)?
   By selecting \( b \) this way, derive a preimage attack which finds a message of length 256b bits for any digest \( h \). (Hint: set \( y = h \oplus H(m) \)).
   What is its complexity?

2 Modulo 11 Diffie-Hellman

1. Let \( d_{n-1}\ldots d_1 d_0 \) be the decimal expansion of an integer \( N \), i.e. \( d_i \in \{0, 1, \ldots, 9\} \) and

\[
N = \sum_{i=0}^{n-1} 10^i \times d_i.
\]

Show that \( N \equiv d_0 - d_1 + \cdots + (-1)^{n-1} d_{n-1} \pmod{11} \).
Deduce an algorithm to reduce an integer modulo 11 by mental computing.
2. What is the order of the \( \mathbb{Z}_{11}^\times \) group?
Show that 2 is a generator of \( \mathbb{Z}_{11}^\times \).
What is the order of 3 in \( \mathbb{Z}_{11}^\times \)?
3. Consider the Diffie-Hellman protocol with prime number $p = 11$ and generator $g = 2$. Alice picks an exponent $x = 9$, sends $X = g^x \mod p$ to Bob and gets $Y = 8$ from him.

Compute $X$.
Compute the Diffie-Hellman key $K$.

3 Modulo 1111 RSA

1. Let $d_{n-1} \ldots d_1 d_0$ be the basis-100 expansion of an integer $N$, i.e. $d_i \in \{0, 1, \ldots, 99\}$ and

$$N = \sum_{i=0}^{n-1} 100^i \times d_i.$$

Show that $N \equiv d_0 - d_1 + \cdots + (-1)^{n-1} d_{n-1} \pmod{101}$.
Deduce an algorithm to reduce an integer modulo 101 by mental computing.

2. With the same notations, show that $N \equiv \sum d_i \pmod{11}$.
Deduce an algorithm to reduce an integer modulo 11 by mental computing.

3. Let $a$ and $b$ be arbitrary integers and let $N = (6 \times 101 \times a + 46 \times 11 \times b) \mod 1111$.
Show that $N \equiv a \pmod{11}$ and $N \equiv b \pmod{101}$.
Show that $N$ is the unique integer with this property in the $[0, 1110]$ interval.

4. Consider RSA signatures with public key $N = 1111$ and $e = 3$.
Compute the secret key $d$.
Compute the signature $y$ of the message $x = 2$. 

2