Isaac Kim
CS 487
Professor Baldimtsi
Apr 16, 2023

Homework 5

1. Let G be $\{0,1\}^n$ under XOR operation.

Closure: Let $g_1, g_2 \in G$. Then, $|g_1| = |g_2| = n$. For all $g_1, g_2 \in G$, $g_1 \oplus g_2 \in G$ since $|g_1 \oplus g_2| = n$.

Identity: Consider $e = 0^n \in G$. Then, for all $g \in G$, $e \oplus g = g$.

Inverse: Let $g \in G$ and $g^{-1} = g$. Then, $g \oplus g^{-1} = 0^n = e$.

Associativity: Let $g_1, g_2, g_3 \in G$. Then, $(g_1 \oplus g_2) \oplus g_3 = g_1 \oplus (g_2 \oplus g_3)$.

Commutativity: Let $g_1, g_2 \in G$. Then, $g_1 \oplus g_2 = g_2 \oplus g_1$.
Hence, G is an abelian group.

2) Using algorithm B.13 from the textbook, 3^{1500} mod 100 can be computed as follows:
Initial variable values: $a = 3, b = 1500, N = 100$

Loop 1: $x = 3, t = 1$, $b = 1500$ is not odd
$t = 1, x = 3^2 \bmod 100 = 9, b = 750$

Loop 2: $x = 9, t = 1$, $b = 750$ is not odd
$t = 1, x = 9^2 \bmod 100 = 81, b = 375$

Loop 3: $x = 81, t = 1$, $b = 375$ is odd
$t = 1 \cdot 81 \bmod 100 = 81, x = 81^2 \bmod 100 = 61, b = (375-1)/2 = 187$

Loop 4: $x = 61, t = 81$, $b = 187$ is odd
$t = 81 \cdot 61 \bmod 100 = 41$, $x = 61^2 \bmod 100 = 21, b = (187-1)/2 = 93$

Loop 5: $x = 21, t = 41$, $b = 93$ is odd
$t = 41 \cdot 21 \bmod 100 = 61$, $x = 21^2 \bmod 100 = 41, b = (93-1)/2 = 46$

Loop 6: $x = 41, t = 61$, $b = 46$ is not odd
$t = 61, x = 41^2 \bmod 100 = 81, b = 46/2 = 23$

Loop 7: $x = 81, t = 61$, $b = 23$ is odd
$t = 61 \cdot 81 \bmod 100 = 41$, $x = 81^2 \bmod 100 = 61, b = (23-1)/2 = 11$

Loop 8: $x = 61, t = 41$, $b = 11$ is odd

$t = 41 \cdot 61 \bmod 100 = 1$, $x = 61^2 \bmod 100 = 21, b = (11-1)/2 = 5$

Loop 9: $x = 21, t = 1$, $b = 5$ is odd
$t = 1 \cdot 21 \bmod 100 = 21$, $x = 21^2 \bmod 100 = 41, b = (5-1)/2 = 2$

Loop 10: $x = 41, t = 21$, $b = 2$ is not odd
$t = 21$, $x = 41^2 \bmod 100 = 81, b = 2/2 = 1$

Loop 11: $x = 81, t = 21$, $b = 1$ is odd
$t = 21 \cdot 81 \bmod 100 = 1$, $x = 81^2 \bmod 100 = 61, b = (1-1)/2 = 0$
Since b = 0, we return $t = 1$. Hence, $\mathbf{3^{1500} \bmod 100 = 1}$.

3) $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$, order = 15.

Let $\mathbb{Z}_{15}^{-1}$ be the set of inverses of the elements in $\mathbb{Z}_{15}$. Then,

$$\mathbb{Z}_{15}^{-1} = \{1, 0, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$$

The i^{th} element of $\mathbb{Z}_{15}^{-1}$ is the inverse of the i^{th} element of $\mathbb{Z}_{15}$. (for all $z_i \in \mathbb{Z}_{15}$ and $z_i^{-1} \in \mathbb{Z}_{15}^{-1}, z_i + z_i^{-1} \bmod 15 = 1$).

Yes, $\mathbb{Z}_{15}$ is cyclic.

4) $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, order = 8.

Let $\mathbb{Z}_{15}^{-1*}$ be the set of inverses of the elements in $\mathbb{Z}_{15}^*$. Then,

$$\mathbb{Z}_{15}^{-1*} = \{1, 8, 4, 13, 2, 11, 7, 14\}$$

The i^{th} element of $\mathbb{Z}_{15}^{-1*}$ is the inverse of the i^{th} element of $\mathbb{Z}_{15}^*$. (for all $z_i \in \mathbb{Z}_{15}^*$ and $z_i^{-1} \in \mathbb{Z}_{15}^{-1*}, z_i \cdot z_i^{-1} \bmod 15 = 1$).

No, $\mathbb{Z}_{15}^*$ is not cyclic.

5)
5.1) Let $k_b = a$ be Bob's key and $k_a = w_3 \oplus t$ be Alice's key. Then, $k_a = w_3 \oplus t = w_2 \oplus b \oplus t = w_1 \oplus t \oplus b \oplus t = w_1 \oplus b = a \oplus b \oplus b = a = k_b$.

5.2) Let A be our adversary/eavesdropper. Then, A can see the transcript which consists of w_1, w_2 and w_3. Note that A does not know what a, b, t are. By Kerckhoff's principle, A knows the process behind generating keys. Then, A can simply compute $w_1 \oplus w_2 \oplus w_3 = (a \oplus b) \oplus (a \oplus b \oplus t) \oplus (a \oplus t) = a \oplus b \oplus a \oplus b \oplus t \oplus a \oplus t = a \oplus a \oplus a \oplus b \oplus b \oplus t \oplus t = a = k$. Since A can compute the key just from the transcript, our protocol is NOT secure.

6)
6.1) $h_a = g^x, h_b = g^y$ for some $x, y \in \mathbb{Z}$.

In class, we did a proof by reduction in which we reduced the Diffie-Hellman protocol to the DDH problem, which states that it is hard for an adversary to distinguish $DH_g(h_1, h_2) = g^{xy}$ from a uniform element of g, given $g, h_1 = g^x, h_2 = g^y, x, y \in \mathbb{Z}$.

Then, even if an eavesdropping adversary eavesdrops on the exchange of g, h_a, h_b, since this problem is hard, (hard to compute $DH_g(h_a, h_b) = g^{xy}$ given g, h_a, h_b), computing $k_A = (g^x)^y = (g^y)^x = k_B$ is also hard. Hence, an eavesdropping adversary cannot simply compute the key.

6.2) To compute $m = Dec(sk, c)$, compute $k = c_1^{sk} = (h_B)^x = (g^y)^x = g^{xy}$. Then, output $m = c_2 \oplus k$. This works because $c_2 = m \oplus k$ (from $Enc(pk, m)$) and so $c_2 \oplus k = m \oplus k \oplus k = m$.