Číslo cvičení: 7
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. Order of any element of the group must be a factor of $\varphi(151) = 150 = 2 \cdot 3 \cdot 5^2$ because 151 is a prime. Denote A set of all integers a such that a is order of some element of $(Z^*_{151}, \cdot)$. We now know that A is a subset of the set of factors of 150. The group is isomorphic to $(Z_{150}, +)$. In the latter group we can easily see that $1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150$ are the orders of $0, 75, 50, 30, 25, 15, 10, 6, 5, 3, 2, 1$.
   The resulting set is therefore $A = \{1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150\}$.

2. $w = -aij^{-1} \mod (p-1)$. Eve can sign only some messages — those which she gets by choosing valid i, j.

3. $S_1 = \frac{1}{2}(\frac{23}{18} + 18) \mod 2011 = 1006 \cdot (23 \cdot 1229 + 18) \mod 2011 = 1071$
   $S_2 = \frac{171}{2}(\frac{23}{18} - 18) \mod 2011 = 171 \cdot 1006 \cdot (23 \cdot 1229 - 18) \mod 2011 = 1084$
   Verification: $1071^2 - 1974 \cdot 1084^2 \mod 2011 = 23$
   Decryption: $\frac{23}{1071 + 171^{-1} \cdot 1084} \mod 2011 = 23 \cdot 1050 \mod 2011 = 18$

4. $0 = k^{-1}(55 + x \cdot 72) \mod 73 \implies 0 = 55 - x \mod 73 \implies x = 55$
   Signing:
   $y = 588^{55} \mod 877 = 546$
   Let $k = 23$.
   $a = (588^{23} \mod 877) \mod 73) = 52$
   $b = 54 \cdot (50 + 55 \cdot 52) \mod 73 = 44$
   Verification:
   $z = 5$, $u_1 = 50 \cdot 5 \mod 73 = 31$, $u_2 = 52 \cdot 5 = 41$
   $(588^{31} \cdot 546^{41} \mod 877) \mod 73 = 52 = a$

5. If H allows calculation of $w \neq w'$, $H(w) = H(w')$, Eve can send w to Alice to be signed by her. Since the hashes are equal and only they are signed, Bob cannot differentiate between signatures of w and w', therefore Eve can send w' to Bob with a valid signature.
   SHA-1 still is considered secure in this notion, since discovery of collisions is computationally unfeasable. The best attacks known today produce collisions in around 2^{60} calculations.

6. (a) $M = 4$, Let $x_1 = 123$, $x_2 = 456$. Let's use the SHA1 hash function.
   $y_1 = H^4(123) = 109861440481732079989047665383404983702139671714 8$
   $y_2 = H^4(456) = 142449010823381824901694657250631905076523210979 3$
   $s_1 = H^3(123) = 103528235806545030565485771565909157116065640082 8$
   $s_2 = H^0(456) = 456$
   $H^1(103528235806545030565485771565909157116065640082 8) = y_1$
   $H^4(456) = y_2$

   (b) Given signed message n, we could sign message $n + 1$ by simply calculating hash of s_1 one more time.

   (c) Computation complexity of this scheme is exponential with respect to N, as opposed to Lamport where it is linear.