# Security

**Assignment 14, Wednesday, January 6, 2016**

**Answers**

1. **(30 points)** Discrete log problems.

   (a) **(10 points)** $11^1 = 11$, $11^2 = 11 \cdot 11 = 35$, $11^3 = 11^2 \cdot 11 = 41$, $11^4 = 11^3 \cdot 11 = 21$, $11^5 = 11^4 \cdot 11 = 16$, $11^6 = 11^5 \cdot 11 = 4$, $11^7 = 11^6 \cdot 11 = 1$ (all mod 43).
   The elements are: 11, 35, 41, 21, 16, 4, 1.

   (b) **(5 points)** $q = 7$.

   (c) **(5 points)** $g^{q+1} = 11^8 = 11$, $g^{q+2} = 11^9 = 35$, $g^{q+3} = 11^{10} = 41$.
   Observation: The elements after $g^q \mod p$ repeat: $g^{q+k} \equiv g^k \mod p$. We are effectively computing modulo $q$ in the exponent.

   (d) **(10 points)** Alternative approach: $21 \cdot 16 \equiv 11^4 \cdot 11^5 = 11^9 \equiv 11^{2 \bmod 7} = 35$. Note that this requires no multiplications at all.

2. **(30 points)** The ElGamal signature scheme.

   (a) **(3 points)** $y = g^x = 3^{21} \equiv 17 \mod 29$

   (b) Solution:

      i. **(3 points)** By Euclidean algorithm, we see that $\gcd(r, p-1) = 1$; the same can be concluded from $5 \not| 28$, since 5 is prime.

      ii. **(3 points)** $s_1 = g^r = 3^5 \equiv 11 \mod 29$

      iii. **(5 points)** $r^{-1} = 17$, since $5 \cdot 17 \mod 28 = 1$. This can be done using egcd (one finds $-11$, and $-11 \equiv 17 \mod 28$):

$$\begin{aligned} 28 - 5 \cdot 5 &= 3 \\ 5 - 1 \cdot 3 &= 2 \\ 3 - 1 \cdot 2 &= 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= 2 \cdot 3 - 5 \\ &= 2 \cdot (28 - 5 \cdot 5) - 5 \\ &= 2 \cdot 28 - 11 \cdot 5 \end{aligned}$$

      iv. **(5 points)** $s_2 = (h(m) - x \cdot s_1) \cdot r^{-1} = (15 - 21 \cdot 11) \cdot 5^{-1} = 8 \cdot 5^{-1} = 8 \cdot 17 = 24 \mod 28$

   (c) Solution:

      i. **(1 points)** $1 \leq s_1 < p$;

      ii. **(5 points)** compute $v := s_1^{s_2} \cdot y^{s_1} = 11^{24} \cdot 17^{11} \equiv \underline{\underline{26}} \mod 29$;

      iii. **(5 points)** $g^{h(m)} = 3^{15} \equiv \underline{\underline{26}} \stackrel{?}{=} v \mod 29$. OK!

3. **(20 points)** Predictable randomness.

   (a) **(5 points)** As we know the public key $y$ and randomness $r$, we can simply compute $y^{-r} \mod p$, and compute $c_2 \cdot y^{-r} \equiv m \cdot y^r \cdot y^{-r} \equiv m \mod p$.

   (b) **(10 points)** The game is similar here. We start by multiplying $s_2$ with $r$ to obtain $H(m) - x \cdot g^r$. We can then subtract $H(m)$, after which we are left with $-x \cdot g^r$, and multiply by $-1$ to obtain $x \cdot g^r$. Now we apply what we used in (a): invert $g^r$ to find $x$, the private key.

   (c) **(5 points)** While breaking an encrypted message reveals that one message, taking apart a signature allows an attacker to derive the long-term secret key. This would then allow for arbitrary signing (and decryption, if the same key was used for both).

4. **(20 points)** Bitcoin. Simply make the transfer and copy the transaction ID. A more nefarious approach would be to look at incoming transactions and simply claim one as your own.