IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises VI.

1. Let $p = 37$, $q = 2$, $y = 17$ be a public key of the ElGamal cryptosystem.
   (a) Encrypt the message $w = 15$, if a random generator gave you $r = 7$.
   (b) Decrypt the message (29,1), if the private key is $x = 7$.
2. Using a primitive root of $\mathbb{Z}_{43}^*$, solve the following congruence
$$x^{19} \equiv 38 \pmod{43}.$$
   Avoid the exhaustive search for a primitive root.
3. Consider any two strongly collision resistant hash functions $h_1 : \{0,1\}^n \to \{0,1\}^m$ and $h_2 : \{0,1\}^n \to \{0,1\}^m$ such that $h_1(x) \neq h_2(x)$ for any $x \in \{0,1\}^n$. Now consider the following hash functions $h : \{0,1\}^n \to \{0,1\}^m$ and $h' : \{0,1\}^n \to \{0,1\}^{2m}$:
$$h(x) = h_1(x) \oplus h_2(x),$$
$$h'(x) = h_1(x) \,||\, h(x).$$
   Determine whether h, h' has to be
   (a) pre-image resistant,
   (b) weakly collision resistant,
   (c) strongly collision resistant.

   Explain your reasoning.
4. Using Shanks' algorithm find x such that
$$11^x \equiv 95 \pmod{97}.$$
   Show the steps of your computation.
5. Consider $n = 103178177$. Factorize n using the knowledge that $7300529^2 \equiv 34404157^2 \equiv 4568721 \pmod{n}$.
6. Consider the Knapsack cryptosystem with a super-increasing private sequence $X = (x_1, \ldots, x_n)$ such that
   (a) $x_1 = 1$,
   (b) $x_i = c2^{i-1}$, $1 \leq i \leq n$, $c > 1$.

   How would such choice affect security?
7. What is the smallest number of people in a group so that the probability that two people in the group have a birthday within the interval of k days is at least $\frac{1}{2}$? Calculate this number for $k = 1, \ldots, 15$.