IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises VI.

1. *(4 points)*
   (a) Encrypt your UČO using the Rabin cryptosystem with $n = 698069$. Then calculate all four possible decryptions of the ciphertext you calculated, with the knowledge that $n = 887 \times 787$.
   (b) Encrypt your UČO with the ElGamal cryptosystem with $p = 567899$, $q = 2$, $x = 12345$ and random choice $r = 938$.

2. *(2 points)* Using baby-step giant-step algorithm find x such that $7^x \equiv 505 \pmod{541}$.

3. *(4 points)*
   (a) What is the probability that at least two students attending IV054 this year have the same birthday?
   (b) What is the probability that another student of IV054 is sharing birthday with you?

   (135 students attend IV054 in 2019.)

4. *(3 points)* Consider a cryptographic hash function with 64 bits long output. Provide an approximate number of random guesses you have to perform to find a collision with probability at least 3/4.

5. *(2 points)* Consider the Blum-Goldwasser cryptosystem with parameters $p = 11$ and $q = 43$. Encode the message $x = 1111$ with $s_0 = 195$.

6. *(4 points)* Determine whether the following functions are negligible. Prove your statement.
   (a) $\ln\left(1 + \frac{1}{n}\right)$
   (b) $e^{1/n}e^{-n}$

7. *(5 points)*
   (a) Suppose you know a valid plaintext-ciphertext pair $w_1 = 457, (a_1, b_1) = (663, 2138)$, constructed using the ElGamal cryptosystem with public key $p = 6661$, $q = 6$, $y = 6015$. Also you know that instead of using a new random r to encrypt each new message, the sender just increments the previous one, i.e. $r_2 = r_1 + 1$. With this knowledge decrypt the following ciphertext $(a_2, b_2) = (3978, 1466)$ without calculating discrete logarithms.
   (b) Show that the same attack is possible for any linear update function of the random seed, i.e. whenever $r_2 = kr_1 + \ell \mod p - 1$.

8. *(6 points)* Consider the following cryptosystem. Let $n = pq$ where p and q are primes. The value n is made public, $(n, \phi(n))$ forms private key.

   Encryption:
   To encrypt a message $m \in \mathbb{Z}_n$, choose a random $r \in \mathbb{Z}_n^*$ and compute
   $$c = (1 + n)^m r^n \mod n^2.$$

   Decryption:
   To decrypt a ciphertext c, compute
   $$m = \frac{(c^{\phi(n)} \mod n^2) - 1}{n} \cdot \phi(n)^{-1} \mod n$$
   where integer division is used.

   (a) Let $n = 3953$. Use $r = 1111$ to encrypt $m = 2019$.
   Decrypt the obtained ciphertext using the fact $n = 59 \times 67$.
   (b) Decrypt $c = 4354044$ without using the private key, only with the knowledge of the plaintext-ciphertext pair from (a).
   (c) Prove the following fact that is exploited in this cryptosystem:
   For integers n and a, $1 \leq a < n$: $(1 + n)^a = 1 + an \pmod{n^2}$.