Biomedical Security

Assignment Set 2

13-9 2018

- Due by 20-9 2018.
- Send your answers in a pdf by e-mail to erwin@liacs.nl
- Use as filename: **<your student number>_<your name>_iBS_Assignment_set_02.pdf**

1. Find a generator *g* of $\mathbb{Z}_{23}^{*}$. Calculate the discrete log of 7 to the base *g* in $\mathbb{Z}_{23}^{*}$.

2. Calculate 9^{27}mod 571 with the fast-exponentiation algorithm. Show the intermediate results in the variables c and d of the algorithm (as given during the last lecture).

3. Find the prime factors of n = 133891. Calculate Euler phi of n: φ(n).

4. Let (e = 77, n = 133891) be the public key of RSA. Give the corresponding secret key of RSA.

5. Calculate gcd(178354,675352).

6. Proof that ElGamal's Public Key Crypto System's decryption step is correct.

7. Proof that the ElGamal's Signature verification step is correct.