

Biomedical Security

Assignment Set 2

8-4 2021

- Due by 20-4 2021, 23.59h.
 - 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 8 to the base g in \mathbb{Z}_{23}^* .
 2. Calculate $9^{83} \bmod 571$ 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 $n = 36349$. Calculate Euler phi of n : $\varphi(n)$.
 4. Let $(e = 77, n = 36349)$ be the public key of RSA. Give the corresponding secret key of RSA.
 5. Calculate $\gcd(178354, 375352)$.
 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.