## Lab 6 – February 2019

a) Two users Alice and Bob want to agree on a secret key over a public network. They have agreed to use the Diffie Hellman algorithm to achieve this. Given the values below what will be the value of the shared secret key generated by Alice and Bob?

| | |
|---|---|
| A random prime | : 11 |
| A generator | : 3 |
| Alice’s random secret | : 4 |
| Bob’s random secret | : 5 |

b) Bad RSA

Using the files listed below can you decrypt the flag

- Badrsa.py
- output.txt

Hint 1

When dealing with RSA encryption, normally cyphertext = (message)^e mod n but in cases where the (message)^e is less than n, then the mod n part of the calculation is ignored. So the ciphertext = (message)^e. If this is the case then the e root of the ciphertext is equal to the message as represented by integers.
*Håstad, Johan (1986). "On using RSA with Low Exponent in a Public Key Network".*
*Advances in Cryptology — CRYPTO ’85 Proceedings. Lecture Notes in Computer Science.* ***218****. pp. 403–408*

Hint 2
https://stackoverflow.com/questions/356090/how-to-compute-the-nth-root-of-a-verybig-integer

Hint 3

https://www.calypt.com/blog/index.php/grehack-write-crypto-300/