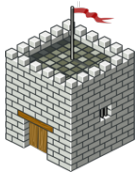
𝔽oundations of Cybersecurity
Exercise Sheet 8
Singapore University of Technology and Design
November 8, 2017



- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Show the solutions of classwork (groups of max 3 persons) to an instructor before the end of the class.
- Submit your homework solutions (groups of max 2) to eDimension by the deadline below.

Classwork due on Wednesday November 8, 10:00 PM

Question 1
Implement the Diffie-Hellman protocol.

Question 2
Implement the RSA encryption scheme from scratch. Use the following interface:
`Gen(minPrime)` generates a public/private keypair where $p, q >$`minPrime`,
`Enc(pubKey, msg)` and `Dec(privKey, ctxt)` both return integers (`msg` and `ctxt` are integers consequently).

Question 3
Implement the RSA signature scheme from scratch. Use the following interface:
`Gen(minPrime)` generates a public/private keypair where $p, q >$`minPrime`,
`Sign(privKey, msg)` returns a signature (integer),
`Verify(pubKey, msg, signature)` returns boolean.
Both, `Sign()` and `Verify()` take `msg` as integer and use a naive hash function `def H(x): return x % 103`.

Homework due on Wednesday November 15, 6:59 PM

Question 1

Let $p = 79, q = 89, n = pq, e = 3$. Is (n, e) a valid RSA public key? If so, compute the corresponding private RSA key d. If not, why not?

Question 2

Compare and report efficiency of your DH and RSA implementations (encryption and signatures) with implementations from a chosen library.

Question 3

Try to conduct timing attacks against your implementation of the RSA encryption: measure time that is needed to encrypt messages with different sizes and contents. What can an adversary deduct about a message given only the execution time of encrypting it? Repeat the measurement for different key sizes.

Question 4

Reimplement your RSA signature scheme, but this time use a real cryptographic hash function, and messages and signatures of the type 'str' (not integers). (You can truncate output of the hash function if it helps you.)