SUTD 51.505: $\mathbb{F}$oundations of Cybersecurity (2018)

Exercise Sheet 10
November 16, 2018

- List your names (max 3 members for each group) on the answer sheet, **if you have actually worked on the exercises.**
- Answer questions in the same order as in the exercise sheet.
- Type in 12pt font, with 1.5 line spacing.
- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Submit your classwork and homework solutions (in pdf file) to eDimension by the deadlines below. Each group only needs one submission.
- Grading: total 100 points for each classwork and homework, each exercise has equal points in the same classwork and homework.

Classwork due on Friday November 16, 10:00 PM

Exercise 1
Implement the Diffie-Hellman protocol.

Exercise 2
Implement the RSA encryption scheme from scratch. Use the following interface:

- `Gen(minPrime)` generates a public/private keypair (512 bits) where $p, q >$ `minPrime`.
- `Enc(pubKey, msg)` returns `ctxt` (integer).
- `Dec(privKey, ctxt)` returns `msg` (integer).

Exercise 3
Implement the RSA signature scheme from scratch. Use the following interface:

- `Gen(minPrime)` generates a public/private keypair (512 bits) 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 SHA-512.

You can choose either Exercise 2 or Exercise 3.

Homework due on Friday November 23, 6:59 PM

Exercise 1

Prove $lcm(a, b) = ab/gcd(a, b)$, where a and b are integers, lcm = the Least Common Multiple, gcd = the Greatest Common Divisor.

Exercise 2

Compute the result of 12358 * 1854 * 14303 (mod 29101) in two ways and verify the equivalence: by reducing modulo 29101 after each multiplication and by computing the entire product first and then reducing modulo 29101.

Exercise 3

What are the subgroups generated by 3, 7, and 10 in the multiplicative group of integers modulo $p = 11$?

Exercise 4

Let $p = 71, q = 89, n = pq, e = 3$. First find the corresponding private RSA key d. Then compute the signature on $m_1 = 5416$, $m_2 = 2397$, and $m_3 = m_1 m_2 \pmod{n}$ using the basic RSA operation. Show that the third signature is equivalent to the product of the first two signatures.

Exercise 5

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.