CSCI971/CSCI471 Modern Cryptography
Spring 2024
Assignment 1 (25 marks)
Due: 01 Sep 2024 23:30

Task A: (5 marks)
Please briefly describe how to break the Monoalphabetic Substitution Cipher. You can refer to the descriptions from the internet but rephrasing is desired.

Task B: (5 marks)
This task is about algorithm definition based on digital signatures. In digital signatures, any user can run key generation to generate a key pair (pk,sk). With sk, the secret key owner can run sign algorithm to generate signatures. With the input pk, message and signature, a verifier can run verification algorithm to verify signatures.

Now, we need a specific signature. Suppose that Alice is the signer and Bob is the verifier. They both have a key pair, namely (pk_A, sk_A) and (pk_B,sk_B). Alice wants to generate a signature such that it can only be verified by Bob who knows the secret key sk_B.

1. What should be added in the **definition** of the signing algorithm and the verification algorithm? (2 marks)
2. Briefly explain why the changes are necessary. (3 marks)

Task C: (5 marks)
What is the output of a 16-round Feistel network when the input is (L,R) and the round function is the identity function (i.e., the function will simply output the input to it). Show the detailed steps in your answer.

Task D: (5 marks)
Let F be a secure blockcipher with block length n. Consider the following message authentication code generation algorithm from F:

MAC. On input a secret key k of F and a message $M \in \{0,1\}^{nl}$, the algorithm first parses M as l blocks $m_1,m_2,\ldots,m_l$. Then it computes $t_i = F_k(m_i)$ for $i \in [1,l]$ and outputs the tag $T=(t_1,\ldots,t_l)$.

Please justify why the scheme is not secure. You should give three different types of attacks.

Task E: (5 marks)
Consider the textbook RSA signature scheme:

- Key Generation:
  - Generate primes P and Q, compute N = PQ.
  - Generate d and e such that de = 1 mod (P-1)(Q-1)
  - Public Key is (N, e) and Private Key is (N,d)
- SIGN:
  - Given message m, compute $s = m^d \bmod N$
- VER:
  - Given message m, signature s, check if $m = s^e \bmod N$

Qa (this question is for CSCI471 students only): Suppose that the adversary is given the signatures on message 3 and 5, describe how to forge the signature for 15 step by step.

Qb (this question is for CSCI971 students only): Suppose that the adversary is given the signatures on message 3 and 5, describe how to forge the signature for 45 step by step.

----------END----------

Submission:

Submit the pdf file to the Moodle site.
The following information should be provided on the top.
The pdf file must be your student number only,such as 55555555.pdf

CSCI971/CSCI471 Modern Cryptography
Assignment 1
Name:_____
Student Number:_____

Plagiarism:
A plagiarised assignment will receive a zero mark (and be penalised according to the university rules).