Modern Cryptography
University of Amsterdam, 2019

Team Name: Your team name
Student Names: Your names

Homework set 1

Contents

Group Project [10 pt]

Invent your own encryption scheme and post it to this discussion forum on Canvas. Note: Only the version submitted to the Canvas discussion forum will be graded, you donâĂŹt have to include it again here. Please make sure that only one person in the team submits.

Clearly specify the following things:

- your team name, and the name of your encryption scheme
- key space, message space, ciphertext space
- Key generation: how to generate keys. You can assume access to a source of truly random bits.
- Encryption: How to encrypt a message given the key.
- Decryption: How to decrypt a ciphertext given the key.
- Correctness: For properly generated keys, the decryption of the encryption of any message gives back this message.
- Security: Argue why it is difficult to decrypt ciphertexts without knowing the key.
- List any advantages and disadvantages of your scheme that you can think of.

Question 1 [4 pt]

Order the following 5 terms according to their asymptotic growth rates.

$$\exp(n), \log(n), n^{\log(n)}, \log(\exp(n)), \exp(\sqrt{n})$$

Solution: Your solution here. Answers have to be fully justified in order to get the full amount of points. □

Question 2 [2 pt]

Use VigenÃÍre encryption to encrypt the message $m =$ `edwardsnowden` with key $k =$ `nsa`. What is the resulting ciphertext c?

Solution: Your solution here □

Question 3 [5 pt]

In logic, contraposition is an inference that says that a conditional statement $A \Rightarrow B$ is logically equivalent to its contrapositive $\neg B \Rightarrow \neg A$. For instance, the proposition "If the weather is good, then I'm biking to work." can be restated as "If I'm not biking to work, then the weather is bad."

State the contrapositives of the following statements:

1. "If the car is broken, it does not drive."
2. "If the weather is nice and I have time, I'm going for a bike ride."
3. "If p is divisible by 8, then p is even."
4. "An attacker can efficiently factorize integers, if he has a large-scale quantum computer."
5. "I love a music album, if in every song, there is a 30-second interval that I like."

Solution:

1. a
2. b
3. c
4. d
5. e

□

Question 4 [2 pt]

Which of the following statements are true about the VigenÃĺre cipher?

1. The VigenÃĺre cipher is computationally infeasible to break if the key has length 100, even if 1000s of characters of plaintext are encrypted.
2. The VigenÃĺre cipher is perfectly secret if the length of the key is equal to the length of the messages in the message space.
3. The VigenÃĺre cipher can always be broken, regardless of the length of the key and regardless of the length of plaintext being encrypted.
4. A VigenÃĺre cipher with key of length 100 can be broken (in a reasonable amount of time) using exhaustive search of the key space.

Solution: □

Question 5 [1 pt]

Let us use a shift cipher on a 10-character alphabet: $\{0, 1, .., 9\}$. Say we have the following distribution over our message space: $\Pr[M = 2] = 0.4$ and $\Pr[M = 6] = 0.6$. What is the probability that the message '6' was encrypted, given that we observe ciphertext '3'?

Solution: □

Question 6 [1 pt]

Consider the VigenÃÍre cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is $\Pr[M = \texttt{aa}] = 0.4$ and $\Pr[M = \texttt{ab}] = 0.6$. What is $\Pr[C = \texttt{bb}]$?

Solution: □

Question 7 [2 pt]

Consider the following encryption scheme: The message space is $M = \{0, \ldots, 6\}$. Algorithm Gen chooses a uniform key from the key space $\{0, \ldots, 7\}$. $\mathsf{Enc}(m)$ returns $[k+m \mod 7]$, and $\mathsf{Dec}_k(c)$ returns $[c-k \mod 7]$. State whether the scheme is perfectly secret and justify your answer.

Solution: □

Programming Question 8 [5 pt]

Watch this video and solve programming assignment 1. Describe the solution and submit your code. You can use an online notebook; for example Google's Colab in case you are using Python.

Solution: □