1. Assignment

Cryptography and Networked Systems Security 2020/2021

Hand-In: Nov. 18th 2019, 10:00

Remarks

(a) Add a statement of contribution.

(b) Groups of 2 to 3 persons are allowed.

Exercise 1 The Dining Cryptographers: Modeling *2+3 points*

Consider the *dining cryptographers* protocol:

> *Three cryptographers are sitting down to dinner at their favorite three-star restaurant. Their waiter informs them that arrangements have been made with the maitre d'hotel for the bill to be paid anonymously. One of the cryptographers might be paying for the dinner, or it might have been NSA (U.S. National Security Agency). The three cryptographers respect each other's right to make an anonymous payment, but they wonder if NSA is paying. They resolve their uncertainty fairly by carrying out the following protocol:*
>
> *Each cryptographer flips an unbiased coin behind his menu, between him and the cryptographer on his right, so that only the two of them can see the outcome. Each cryptographer then states aloud whether the two coins he can see–the one he flipped and the one his left-hand neighbor flipped–fell on the same side or on different sides. If one of the cryptographers is the payer, he states the opposite of what he sees. An odd number of differences uttered at the table indicates that a cryptographer is paying; an even number indicates that NSA is paying (assuming that the dinner was paid for only once). Yet if a cryptographer is paying, neither of the other two learns anything from the utterances about which cryptographer it is.*

Assume a cryptographer is paying. Our goal is to provide a precise definition of the last sentence: *Yet if a cryptographer is paying, neither of the other two learns anything from the utterances about which cryptographer it is.*

(a) Model the above as probability space by giving a set of elementary events Ω, and provide random variables for all exchanged keys, the "plaintext" (the bit of information whether a particular cryptographer is paying or not), and the "ciphertext" (the bit of information each cryptographer says out loud).

(b) Give a precise mathematical definition, what it means for the paying cryptographer to be "anonymous" against the other non-paying cryptographers. *Hint: look at one non-paying cryptographer and take his knowledge into account.*

Exercise 2 Caesar Cipher *1+2+1+1 points*

Recall the caesar cipher (resp. *shift cipher*), where a letter is encrypted by replacing it with the one with distance 3 in the alphabet.

(a) Generalize the caesar cipher to support a private key (the distance in the alphabet is the key) and write it down as private key encryption scheme (i.e. provide G, E and D).

(b) This shift cipher operates on single letters. Model a probability space for eavesdropping on a single ciphertext letter and specify random variables M for the plaintext, K for the selected key and C the ciphertext.

Adapt (if necessary) this probability space for longer messages and specify random variables M_i and C_i for the i-th letter in the plaintext resp. ciphertext.

(c) Implement a small utility, that, on input a text string, outputs the relative frequency of letters in that string. Now, assume you intercepted the ciphertexts:

```
wkhtxlfneurzqiramxpsvryhuwkhodcbgrj
```

and

```
svkceboyrzdhvpxyljvgutnyinavmrqwrgf
```

(a) Do both messages encrypt the same message?

(b) Decrypt the former. What is the secret key? **Hint:** the source language is english.