Lista 1 - Criptografia

João Pedrosa

1 de Junho de 2021

1 Review Questions

1. **What is the definition of Cryptography according to your teacher? What is the essential difference between cryptography and distributed algorithms**?

   Criptografia é a área de segurança da informação que faz uso de ferramentas matemáticas para alcançar uma comunicação segura entre dois agentes, mesmo na presença de adversários. Na maioria das vezes, os dois agentes estão geograficamente separados e utilizando um canal inseguro para comunicação. Algoritmos disribuídos são algoritmos rodados por diferentes agentes que confiam uns nos outros, para atingir algum objetivo.

2. **What is the definition of a cryptographic protocol? Which protocol plays the most important role in cryptography?**

   Um protocolo criptográfico é um algoritmo distribuído, com a diferença de que os agentes que o executam não confiam uns nos outros. Os protocolos mais importantes são os de encriptação e decriptação de dados.

3. **What is the definition of a cryptographic algorithm? Give some examples.**

   Algoritmos criptográficos são os algoritmos utilizadas como meio para alterar as mensagens de um formato legível para um formato seguro. Alguns exemplos são os algoritmos de encriptação e decriptação, os algoritmos de verificação de assinaturas e as funções de hash.

2 Exercise

1. **Explain or, ideally, prove formally that the protocol preserves the privacy of each bank.**

   O protocolo funciona pois todos os valores r se cancelam na soma final. Entretanto, cada banco sabe apenas os valores que ele enviou e que ele recebeu, não sabendo os valores que os outros bancos compartilharam entre si. Sendo assim, nenhum dos bancos possui informação o suficiente para calcular os valores de x sabendo apenas os valores de y.

2. **Could this protocol be executed with 2 banks? With 3? Why (not)?**

   O protocolo não funcionaria com apenas 2 bancos. Ambos os bancos saberiam todos os valores de r, afinal, os únicos 2 valores que existiriam seriam o valor que o banco 1 enviou para o 2 e o valor que o banco 2 enviou para o 1. Com 3 bancos seria possível pois cada um dos bancos não saberia 2 valores, eg. o banco 1 não saberia o valor que o banco 2 enviou para o banco 3, nem o valor que o banco 3 enviou para o banco 2.

3. **Is this protocol secure if the banks do not agree on an upper bound beforehand? Explain.**

4. **Now the banks need to vote on some topic, so someone suggest the following solution: $No = 0, Yes = 1$, and use the preceding protocol to sum the votes. Why is such a voting scheme in most context not a good idea? What is the difference compared to the computation of the sum?**

5. **Give a protocol specification for the Coin Flipping (CF) protocol using bits and the xor operation (addition mod 2), instead of coin flip results and equal or different.**

   Alice escolhe um bit aleatório a, encripta ele com uma função Com tal que $Com(a) = c$ e envia c para Bob. Bob escolhe um bit aleatórib b. Em seguida, definimos $f(a, b) = aXORb$. Se $f(a, b) = 1$, então Alice ganha. Se $f(a, b) = 0$, então Bob ganha.

6. **Prove (the) CF (protocol) secure for Alice. State the property you need to prove and the underlying assumption(s). Try to be as formal as possible, but if you have difficulties then describe your arguments in words.**

   Assumindo que seja impossível que Bob descubra qual o valor de a, sabendo apenas o valor de c:

   Bob saberá o valor escolhido por Alice, apenas após escolher seu próprio valor, portanto, é fácil perceber que Bob não teria nenhuma vantagem em escolher um valor ou outro e, sendo assim, o protocolo é seguro para Alice.

7. **Prove (the) CF (protocol) secure for Bob. State the property you need to prove and the underlying assumption(s).**

   Assumindo que Alice irá passar uma função de decriptação verdadeira para Bob após Bob ter escolhido seu valor:

   Bob escolhe o seu valor após Alice já ter feito a escolha do valor dela. Portanto, não existe benefício em Alice escolher um valor ou outro e, sendo assim, o protocolo é seguro para Bob.

8. **Explain how you would create a Bit Commitment scheme given a cryptographic hash function like MD5, SHA1, SHA256 (these**

will be discussed extensively later in the course). How do you deal with an adversary trying to guess a 0 or a 1?

9. **Discuss how Protocol 1.1 in [Mao, pag. 5] is different from the slides. Observe that a hash function could play the role of Mao's 'magic function'.**

10. **Give a high-level description of a ZK protocol for showing knowledge of a solution to a sudoku puzzle. See page 64 of this article for inspiration.**

    Alice tem uma solução para o Sudoku e quer convencer Bob que existe solução, sem contar para ele qual solução é. Bob irá jogar 9 moedas, ou, paralelamente, escolher 9 bits b. Para cada b_i, se $b_i == 1$, Alice mostra para Bob a solução da coluna i do Sudoku. Bob ao final pode checar que nenhuma coluna e nem linha que Alice passou, tem números repetidos. Da mesma forma, Alice sabe que Bob ainda não tem total informação acerca do Sudoku, a não ser que todas os b sejam iguais a 1. A chance de Alice se dar mal é de $\frac{1}{2^9}$.