
The University of Queensland
School of Information Technology and Electrical Engineering
Semester Two, 2011

COMS3200 – Tutorial 12

Questions

1. Compare (in general terms) the DES and RSA algorithms.
2. Explain why sending $\mathbf{m} + \mathbf{MD5}(\mathbf{m})$, which denotes message \mathbf{m} concatenated with its digest, does not guarantee message integrity for \mathbf{m} . What can you do make it secure?
3. What is the reason for the existence of Certification Authorities?
4. The SSL data transport protocol involves two nonces (random numbers) as well as premaster key. What purpose, if any, does using the nonces have?
5. Perform encryption and decryption using RSA as explained in the Lecture for the following: $p=3$, $q=11$, $e=7$, $M=5$.
6. Alice wants to communicate with Bob, using public-key cryptography. She establishes a connection to someone she hopes is Bob. She asks him for his public key and he sends it to her in plaintext along with a certificate signed by the root CA. Alice already has the public key of the root CA. What steps does Alice carry out to verify that she is talking to Bob? Assume that Bob does not care who he is talking to (e.g. Bob is some kind of public service).
7. This question is optional. (Only for the keen cryptographer!)
Break the following monoalphabetic substitution cipher. The plaintext, consisting of letters only, is from a well-known poem by Lewis Carroll.
Hint: The word “carpenter” appears in the plaintext.
The following applet might also help:
http://www.wiley.com/college/mat/gilbert139343/java/java11_s.html

kfd ktbd fzm eubd kfd pzyiom mztX ku kzyg ur bzha kfthcm
ur mfudm zhx mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm
zhx pfa kfd mdz tm sutythc fuk zhx pfdkfdi ntem fzld pthcm
sok pztk z stk kfd uamkdim eitdx sdruid pd fzld uoi efzk
rui mubd ur om zid uok ur sidzfk zhx zyy ur om zid rzk
hu foiaa mztX kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk