

COMS3200 – Tutorial 12 Solutions

Questions

1. Compare (in general terms) the DES and RSA algorithms.

DES uses a secret key shared between two communicating entities (which creates a problem of key distribution). DES is a substitution algorithm where 64 bits of plaintext are substituted with 64 bits of ciphertext (yielding always the same result if the algorithm is repeated on the same plaintext) - this feature changes if block chaining is used. There is no mathematical proof of DES security. Its security is based on its complexity - the key space has to be searched to break the encryption. DES is a fast algorithm. There are hardware implementations of DES. RSA uses two keys, public and private. Public key is used for encryption and private for decryption (the process is reversed for creating digital signatures). Certificates are necessary for public key distribution to ensure that public keys are legitimate. The RSA algorithm is grounded in number theory. There is no mathematical proof of RSA security. Its security is based on the difficulty of factoring large numbers. It is considered very secure when long keys are used. The algorithm is computationally expensive and is suitable only for short messages (e.g. to support distribution of keys for DES).

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 to make it secure?

An intruder may intercept m , change its content and compute MD5 on the new content. The receiver will not be able to detect that such modification has happened. However, if the digest is computed from the message m and a secret key k (shared between sender and receiver), no third party without the key k would be able to recompute a valid digest on a changed message. The sender will send the following: $\mathbf{m} + \mathbf{MD5}(\mathbf{m}, \mathbf{k})$

3. What is the reason for the existence of Certification Authorities?

Public keys are public therefore they do not need to be distributed securely as DES keys have to be. It is necessary, however, to prove that the public key belongs to the entity that it claims to belong. A certificate simply links a public key to an identity.

-
- The SSL data transport protocol involves two nonces (random numbers) as well as premaster key. What purpose, if any, does using the nonces have?

The nonces guard against replay attacks. Since each party contributes to the key, if an intruder tries to replay old messages, the new key generated will not match the old one.

- Perform encryption and decryption using RSA as explained in the Lecture for the following: $p=3$, $q=11$, $e=7$, $M=5$.

First, we need to find the private key d . We know that the following must hold:
 $ed \bmod z = 1$

$$z = (p-1)(q-1) = 2 \cdot 10 = 20$$

therefore: $7d \bmod 20 = 1$

We can easily see that $d=3$.

(For large p and q , finding d is not that trivial. However, there exist efficient algorithms to compute d if p and q are given. No efficient (polynomial) algorithm is known to compute d if only n is known but not its prime factors p and q . The security of RSA therefore relies on the fact that there is no known efficient algorithm to factor large numbers.

Encryption:

$$C = M^e \bmod n = 5^7 \bmod 33 = 78125 \bmod 33 = 14$$

Decryption:

$$M = C^d \bmod n = 14^3 \bmod 33 = 2744 \bmod 33 = 5$$

- 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).

Step 1 is to verify the certificate using the root CA's public key. If it is genuine, she now has Bob's public key. (She should check the (Certificate Revocation List) CRL if there is one.) But to see if it is Bob on the other end of the connection, she needs to know if Bob has the corresponding private key. She picks a nonce and sends it to him with his public key. If Bob can send it back in plaintext, she is convinced that it is Bob.

-
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 mztz 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 ncm fzld pthcm
sok pzk z stk kfd uamkdim eitdx sdruid pd fzld uoi efzk
rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk
hu foiaa mztz kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

Plaintext:

the time has come the walrus said to talk of many things
of shoes and ships and sealing wax of cabbages and kings
and why the sea is boiling hot and whether pigs have wings
but wait a bit the oysters cried before we have our chat
for some of us are out of breath and all of us are fat
no hurry said the carpenter they thanked him much for that