TTM4135 final exam May 2015: outline answers

Written answer questions

1. The description should describe how substitution replaces sub-blocks in the state; permutation moves around each bit of the block state; sub-key is XOR added to current block state.

2. Since the nonce N is fixed it means that the values O_t are the same for each message. In a known plaintext attack the attacker knows P_t and C_t for each t and can therefore obtain the O_t values by simply computing $O_t = P_t \oplus C_t$. Then for another message $P_1', P_2', \ldots$ the attacker can obtain $P_t' = O_t \oplus C_t'$.

3. (a) An attacker who can factorise n obtains p and q and can therefore compute $\phi(n) = (p - 1)(q - 1)$ and hence obtain the private key $d = e^{-1} \bmod \phi(n)$.

   (b) Reasonable choices are between 1024 and 2048 bits. It should be noted that too large modulus affects efficiency badly, while lower than 1024 risks factorisation. Realistic quantum computers will make factorisation polynomial time and there is no practical size which can work any longer.

4. (a) If (r, s) is a valid signature then $m = ks + xr \bmod (p - 1)$ and so $g^m = g^{(ks+xr)} = g^{ks}g^{xr} = r^s y^r$.

   (b) The adversary will see two signatures (m_1, r, s_1) and (m_2, r, s_2) where $r = g^k \bmod p$ and $s_1 = k^{-1}(m_1 - xr) \bmod (p - 1)$, $s_2 = k^{-1}(m_2 - xr) \bmod (p - 1)$.
   Therefore $s_1 - s_2 = k^{-1}(m_1 - m_2)$ or $k = \frac{m_1 - m_2}{s_1 - s_2} \bmod (p - 1)$. Now that k is found the adversary can compute $x = r^{-1}(m_1 - ks_1) \bmod (p - 1)$.

5. (a) Take $a = 2$ then we need to see that $2^{22} \bmod 23 = 1$. $2^4 \equiv 16 \equiv -7$ so $2^8 \equiv 49 \equiv 3$. Then $2^{16} \equiv 9$. $2^6 \equiv 64 \equiv -5$. Thus $2^{22} \equiv 9 * -5 \equiv -45 \equiv 1$.

   (b) The Fermat test for a number n is to check whether $a^{n-1} \bmod n = 1$ for a random a. If not then n is composite. If so then repeat with further a. $2^4 \bmod 15 \equiv 1$. Therefore $2^{12} \bmod 15 \equiv 1$ and so $2^{14} \bmod 15 \equiv 4 \neq 1$. So the test recognises that 15 is composite.

6. (a) Both a MAC and a hash function take a message of (practically) any size and output a tag or digest. However, a MAC includes also a key in the calculation so that computation of the correct tag requires knowledge of the key.

   (b) If a hash tag were used instead of a MAC it can be computed by anybody. An attacker could change a transmitted value in any desired way and compute the correct hash itself.

7. (a) Nonce N_1 is used to prevent replay attacks. It is generated by C and returned in the message from AS cryptographically bound to the key $K_{C,tgs}$. C will check that the value returned is the same as it sent in the first message. This allows C to verify that this key is not replayed from a previous run of the protocol.

   (b) ID_{tgs} is checked by C to ensure that the key returned from AS is valid for the correct (ticket granting) server. If it were omitted then an attacker could change the identity in the first message before it got to AS and then C would accept the key for the wrong server.

8. The handshake protocol will use RSA to transport the pre-master key from the client to the server. The record protocol will use AES with 128-bit key and CBC mode of operation and also SHA-256 for HMAC construction.