Solver: Zhou Zhiyao

Email Address: zhou0250@e.ntu.edu.sg

1. (a) False. Symmetric key cryptography is more efficient for large amount of data.
   (b) False. Fundamental difference is that AES is not based on Feistel structure.
   (c) True. By computation.
   (d) False. $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$
   (e) False. Set-up 1 is weaker because it is susceptible to meet-in-the-middle attack.
   (f) False. Hash may not be of 256 bits.

2. (a)
   $(x^2 + 1)(x^4 + x^3 + x^2 + x) + (x^6 + x^5 + x^2 + x + 1) = 1$
   $x^4 + x^3 + x^2 + x$ is the multiplicative inverse of $x^2 + 1$

   (b)
   $19^3 \ mod \ 5 = 4$
   $19^3 \ mod \ 7 = 6$
   $\mathrm{A} = 19^3 \ mod \ 35 \leftrightarrow (4,6)$

   $\mathrm{M} = 35 = m_1 \times m_2 = 5 \times 7$
   $7 \times 3 \bmod 5 = 1$
   $5 \times 3 \bmod 7 = 1$
   $c_1 = 7 \times 3 = 21, \ c_2 = 5 \times 3 = 15$

   $\mathrm{A} = \left(\sum_{i=1}^{k} a_i c_i = 4 \times 21 + 6 \times 15 \right) mod \ 35 = 174 \bmod 35 = 34$

3. (a)
   During phase 4 of handshake protocol when change cipher specification

   (b)
   (i)
   1. C intercept the message A sends to B: $\mathrm{E}(PU_B, N_A)$, A and forward to B
   2. C change the message to: $\mathrm{E}(PU_B, N_A)$, C and start a new session with B
   3. B sends back: $\mathrm{E}(PU_C, (B, N_A + 1))$
   4. C knows the session key of A and B $\mathrm{h}(N_A)$

   (ii)
   (A) does not solve the issue, attacker can still send a modified message to get N.
   (B) does not solve the issue, attacker can send a modified message with his own signature to get N.

(C) solves the issue. Now the identity of sender and N is encrypted together in the message. The attacker cannot fake the message by the method in Q3(b)(i).

4. (a)
It is needed to ensure freshness.

(b)
Since the hash function uses Merkle-Damgard construction, the attacker can apply length extension attack.
To construct the MAC for M1+M2

$\mathrm{E}(\mathrm{K}, M_2) = b_1 b_2 \ldots b_n$
$\mathrm{MAC}(\mathrm{K}, M_1 + b_1) = \mathrm{f}(\mathrm{MAC}(\mathrm{K}, M_1), b_1)$
$\mathrm{MAC}(\mathrm{K}, M_1 + b_1 + \cdots + b_i) = \mathrm{f}(\mathrm{MAC}(\mathrm{K}, M_1 + b_1 + \cdots + b_{i-1}), b_i)$
$\mathrm{MAC}(\mathrm{K}, M_1 + M_2) = \mathrm{f}(\mathrm{MAC}(\mathrm{K}, M_1 + b_1 + \cdots + b_{n-1}), b_n)$

(c)
In step (4), A has no way to determine if k and N3 is fresh.
If the attacker knows a past $\mathrm{E}(K_{AB}, (\mathrm{k}, N_3))$, he can just forward messages in the first three steps between A and B then replay $\mathrm{E}(K_{AB}, (\mathrm{k}, N_3))$ to A.
A will accept the old k and start sending secret message with session key k.

For reporting of errors and errata, please visit pypdiscuss.appspot.com
Thank you and all the best for your exams! ☺