Provide in-depth answers (7-8 lines)

1. What is DNS cache poisoning? How is this typically achieved by an attacker?

2. How does DNSSEC address cache poisoning attacks?

3. Provide a brief (5 to 6 lines) justification as to why one should use SSL.

4. In PGP it was argued that authenticate (sign)- compress – encrypt is the desirable sequence. For SSL records the order is however compress – authenticate (add MAC) – encrypt. Explain.

5. Explain the need for dual signatures in SET. How is this achieved?

6. State True or False. Provide an one-line explanation.
   (a) Cookies can be used for phishing personal information from users

   (b) When DNSSEC is used the DNS server s sign every DNS response

   (c) If DNS queries did not carry sequence numbers, attackers will not need to run their own DNS servers to poison the cache of other DNS servers

   (d) The payload of SSL record packets is TCP packets (TCP packets are carried by SSL record packets)

   (e) Phase 3 of SSL handshake is optional when DNSSEC is used.