

# 2014 augustus examen

1. Het verschil tussen ECB en CBC en waarom dat het een beter is dan het andere
2. Waarom dat P2P beter is in het distribueren van files dan client-server
3. Prefetchen uitleggen
4. Kan er gezegd worden dat een CA een "Trusted Third Party" is bij PKI
5. Leg onweerlegbaarheid uit bij het gebruik van PGP
6. Het belang van een nonce binnen authenticatie
7. Wat is de cryptografische functie van een CA
8. Het verschil tussen end-to-end vertraging en pakketjitter
9. Waar/Niet waar + Uitleg
  1. Kan Jitter (Variatie Delay) opgelost worden door gebruik te maken van QoS
  2. Als een hacker de Publieke Sleutel van een website in handen krijgt heeft deze toegang tot alle sessies, en alle voorgaande sessies als deze werden opgenomen (Sniffing)
  3. Een Packet-filter kan geen virussen tegenhouden
  4. Voorbeelden van applicatie gateway zijn web cache en een server
  5. Als je zo snel mogelijk een bestand wil versturen naar een verre locatie (+15 hops) dan gebruik je TCP
  6. Er zijn minder regels bij een packetfilter om een bepaalde TCP communicatie toe te staan tussen client-server dan bij stateful inspection firewall
  7. In een DMZ (Demilitarized Zone) staan geen interne servers
  8. Bij VoIP loopt verkeer van alle gesprekken via de SIP proxys
  9. Een systeem dat gebruikt maakt van HMAC is gevoelig voor replayaanvallen

---

Revision #1

Created 17 June 2021 12:07:35 by Jasper G.

Updated 3 December 2021 22:13:08 by Jasper G.