

Oefenopgaven Security

Onderstaande vragen dienen slechts om een niet uitputtende indruk te geven van vragen die op de toets kunnen voorkomen.

1. Hoeveel mogelijkheden heeft een wachtwoord met een lengte van 10 tekens dat samengesteld mag worden uit hoofdletters, kleine letters en 10 overige leestekens?
2. Ontsleutel m.b.v. Vigenere encryptie en de sleutel 'proeftoets' de boodschap 'LVCRYFCIMWCYSXABSVWWJLFMSWSENDP'
3. Schrijf uit hoe Alice en Bob met behulp van Diffie-Hellman bij hun sleutels uitkomen wanneer ze overeenkomen dat $p = 31$ en $g = 2$.
4. Wat is het verschil tussen een worm en een virus?
5. Wat is het verschil tussen HTTP en HTTPS?
6. Leg uit hoe webcertificaten werken
7. Wat is een *dictionary attack*?
8. a) Creëer een RSA sleutelbaar met $p=13$ en $q=19$
b) Versleutel het getal 55 met de ene sleutel en ontcijfer de uitkomst met de andere sleutel.
9. a) Creëer een RSA sleutelbaar met $p=53$ en $q=97$
b) Versleutel het getal 121 met de ene sleutel en ontcijfer de uitkomst met de andere sleutel.