Ishod 3 (12 bod, 30 min)

1. **(1) Što je kriptologija?**

Znanost koja se bavi sigurnom komunikacijom, a uključuje kriptografiju i kriptoanalizu.

2. **(1) Hakeri su upali u sustav i pokupili sve podatke o korisnicima (uključujući i njihove zaporke). Koja mjera vas može donekle spasiti? Objasnite zašto.**

Mjera koje može pomoći je hashiranje lozinki (Argon2). Hash je vrlo teško obrnuti bez poznavanja stvarne lozinke.

3. **(1) Objasnite Cesarovu šifru te navedite kojoj tehnici šifriranja pripada.**

Jednostavna tehnika šifriranja gdje se svako slovo zamjenjuje slovom koje se nalaze određeni broj mjesta dalje u abecedi. Pripada tehnici zamjene.

4. **(1,5) Objasnite kako rade algoritmi sažimanja. Što znači otpornost na kolizije za dani algoritam sažimanja? Navedite primjere korištenja.**

Algoritmi sažimanja pretvaraju proizvoljno velike ulazne podatke u fiksno velik niz znakov.
Otpornost na kolizije znači da je teško pronaći dva različita ulaza s istim izlazom.
Primjeri korištenja: verifikacija lozinki, digitalni potpisi

5. **(2) Kratko objasnite simetričnu i asimetričnu enkripciju? Koje su prednosti i nedostaci? Navedite najčešće primjene.**

Simetrična enkripcija koristi isti ključ za enkripciju i dekripciju.
Prednost: brza i jednostavna
Nedostatak: potrebno je sigurno podijeliti ključ
Primjer: enkripcija diska

Asimetrična enkripcija koristi javni i privatni ključ
Prednost: jednostavno uspostavljanje sigurnosti kanala komunikacije
Nedostatak: spor i složen
Primjer: PGP email enkripcija

6. **(1) Objasnite na primjeru TLS-a kako se koristi simetrična i asimetrična enkripcija zajedno.**

TLS koristi simetričnu enkripciju za prijenos podataka (brzina), a asimetričnu enkripciju za sigurno dijeljenje ključeva (sigurnost).

7. **(2) Objasnite pojam PKI. Što je neporicivost i autentičnost? Na koji način je to omogućeno u PKI infrastrukturi?**

Public Key Infrastructure je sustav za izdavanje, upravljanje i pohranu javno-privatnih ključeva i digitalnih certifikata.

Neporecivost - dokaz tko je poslao podatke (zbog digitalnog potpisa)

Autentičnost - potvrđivanje identiteta korisnika sustava (omogućeno verifikacijom certifikata izadnog od CA)

8. **(1,5) Što je root CA i čemu služi te objasnite učinkovite kontrole za zaštitu root CA?**

Glavna organizacija koja izdaje digitalne certifikate kojima vjeruju svi korisnici.
Zaštita root CA uključuje fizičko čuvanje, air-gap izolacije, rijetkog korištenja i višefaktorskih kontrola pristupa.

9. (1) Je li moguće probiti AES algoritam? Objasnite.

Advanced Encryption Standard je trenutno smatran sigurnim i praktički neprobojan uz pravilnu implementaciju i koristi dovoljan dugačak ključ od 128, 192 ili 256 bitova.

Dodatno

Što je digitalni certifikat? Navedite najčešće primjene korištenja.

Digitalni certifikat je elektronički dokument koji vezuje javi ključ sa identitetom. Najčešće primjene su web stranice.

Što je kriptoanaliza?

Disciplina koja se bavi razbijanjem šifru bez ključa za dekripciju.

Koje podjele kriptografskih algoritama postoje?

Simetrična, asimetrična, algoritmi sažimanja, Digitalni potpis, ...

Što je kriptografija?

Znanost koja se bavi zaštitom informacija putem matematičkih metoda.