2. Zadaća iz predmeta "Zaštita i sigurnost informacijskih sustava"

4-11 Što je od navedenog ispravna izjava koja se odnosi na enkripciju podataka kada se ona koristi za zaštitu podataka ?

A. Verifikacija integriteta i točnosti podataka
B. Zahtijeva se pažljivo upravljanje ključevima
C. Ne zahtjeva se mnogo sistemskog overhead-a u potrebnim resursima
D. Zahtjeva se da se ključevi založe

4-12 Ako različiti ključevi generiraju isti šifarski tekst za istu poruku kako se to naziva ?

A. Kolizija
B. Sigurni hash
C. MAC
D. Grozd ključeva (key clustering)

4-13 Koji je glavni razlog za uvođenje jednosmjerne enkripcije (one way encription) korisničkih lozinki?

A. Minimiziranje prostora na hard disku i sistemskim resursima za pristup lozinkama
B. Izbjegavanje intenzivnog korištenja vremena obrade koje se zahtjeva upotrebom simetrične enkripcije
C. Sprečavanje čitanja lozinki u čistom tekstu
D. Osiguranje pristupa datoteci lozinki za potrebe nadzora

4-14 Koje servise osiguravaju ESP i IPSec protokoli ?

A. Autentifikaciju i raspoloživost
B. Povjerljivost i integritet
C. Raspoloživost i povjerljivost
D. Kontrolu pristupa i raspoloživost

4-15 Što je od navedenog najranjivije na napad 'man-in-the midlle' ?

A. Protokoli za izmjenu ključeva
B. Algoritmi simetričnih klj učeva
C. IPSec protokol
D. S/MIME (secure mail)

5-15 Certifikacijsko tijelo (CA) može delegirati jedan od slijedećih procesa:

A. Opoziv i suspenziju pretplatničkog certifikata
B. Generiranje i distribuciju javnog ključa od CA
C. Uspostavu veze između entiteta koji zahtjeva certifikat i njegovog javnog ključa
D. Izdavanje i distribuiranje pretplatničkog certifikata

5-16 Što od navedenog daje najveću sigurnost u autentifikaciji poruke ?

A. Prethodni hash kod se dobiva matematički iz poruke koja se odašilje
B. Prethodni hash kod se kriptira koristeći privatni ključ pošiljaoca poruke
C. Prethodni hash kod i poruka se kriptiraju koristeći tajni ključ
D. Pošiljalac uzima javni ključ primaoca i verificira autentičnost njegovog certifikata sa CA

5-17 Što od navedenog osigurava uslugu neporecivosti za e-commerce transakcije ?

A. Infrastruktura javnog ključa (PKI)
B. Dana Encryption Standard (DES)
C. Message autentication code (MAC)
D. Personal identification number (PIN)

5-18 Uloga certifikacijskog tijela (CA) kao treće strane je:

A. Osigurava sigurnu komunikaciju i mrežne servise temeljene na certifikatima
B. Smještaj repozitorija certifikata sa odgovarajućim javnim i tajnim ključevima koji su izdani od tog CA
C. Aktivno učešće (medijator) u povjerljivoj komunikaciji između partnera
D. Potvrda identiteta vlasnika certifikata koji je izdao ovaj CA

5-19 Koja od navedenih izjava ispravno opisuje biometrijske metode ?

A. One su najjeftinije i najsigurnije
B. One su najskuplje i najmanje sigurne
C. One su najjeftinije i najmanje sigurne
D. One su najskuplje i najsigurnije