1. **Co je to elektronická značka**
   a) Technologicky totéž co zaručený elektronický podpis
   b) Ověření elektronické značky je obtížnější než ověření elektronického podpisu
   c) Liší se od elektronického podpisu jen režimem použití soukromého klíče
   d) Elektronická značka je ke zprávě připojena tak, že je možné detekovat následné změny ve zprávě

ACD

2. **Forenzní řešení biometrik popisují tyto výroky**
   a) cena je vysoká, ale s tím se počítá.
   b) výsledek autentizace je získán obvykle za 1s či rychleji.
   c) miniaturizace zařízení je jedním z hlavním cílů.
   d) pro používání je nutná odborná znalost systému.

AD

3. **Vhodná tajná informace pro autentizaci je**
   a) Fráze (passphrase)
   b) Rodné příjmení matky
   c) Heslo
   d) PIN
   e) Tel. číslo, pokud není uvedeno ve Zlatých stránkách

ACD

4. **Biometrické technologie mohou být založeny na některém z těchto typů charakteristik:**
   a) behaviorální
   b) chemoterapický
   c) morální
   d) fyziologický
   e) environmentální

AD

5. **Co je to narozeninový paradox?**
   a) Pravděpodobnost nalezení stejného data narození k pevně zvolenému datu je při 23 lidech větší než 50 %
   b) Situace, kdy se začátkem roků rodí víc mužů než žen
   c) Statisticky podložená vysoká úspěšnost nalezení kolize
   d) V sále s 23 lidmi je pravděpodobnost stejného data narození dvou lidí větší než 50 %

CD

6. **Detekcí narušení se u čipových karet myslí:**
   a) Vlastnost části systému umožňující detekovat fyzický útok.
   b) Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
   c) Při zjištění narušení je automaticky provedena chráněnou části obranná akce.
   d) Po narušení jsou stopy narušení obtížně odstranitelné.

A

7. **Každá z dvou komunikujících stran má svůj symetrický klíč. Kolik zpráv se vymění ve Shamirově protokolu bez klíčů, aby obě strany sdílely stejný klíč?**
   a) žádná z těchto odpovědi není správná
   b) 2
   c) 3
   d) 4

C

8. Které z uvedených možností zajišťuje protokol Ipsec?

a) Podporu správy klíčů.
b) Nepopiratelnost přijetí dat.
c) Autentizace a integrita původu dat.
d) Důvěrnost dat, ochrana proti útoku přehráním.

ACD

9. Mezi vlastnosti (axiomy) modelu Bell-LaPadula patří

a) procesy nesmějí zapisovat data do nižší úrovně
b) procesy nesmějí číst data z nižší úrovně
c) procesy nesmějí číst data na vyšší úrovni

AC

10. Jaká jsou platná tvrzení pro aktivní autentizaci elektronických pasů?

a) Soukromý klíč je uložen v čipu, bez možnosti jeho přímého získání
b) Veřejný klíč je uložen ve čtečce el. pasů a je digitálně podepsán
c) Pro autentizaci je použit zero-knowledge protokol (Fiat-Shamir), který zároveň ověří, zda má pas dispozici soukromý klíč
d) Protokol výzva-odpověď lze použít pouze pokud čip neumožňuje efektivní implementaci zero-knowledge protokolu

A

11. Z hlediska lidské paměti je vhodné volit

a) Složitá, ale snadno zapamatovatelná hesla
b) Jednoduchá a jednoduše zapamatovatelná hesla
c) Obtížně zapamatovatelná hesla a každý měsíc nutit uživatele ke změně
d) Hesla založená na frázích

ABD

12. Pro autentizaci obrazovou informací platí

a) Uživatel musí systému slovně popsat obrázek sloužící k autentizaci
b) Uživatel musí vybrat správný obrázek nebo jeho část
c) Uživatel musí do systému nahrát správný obrázek
d) Uživatel musí správně vybarvit předložený obrázek

B

13. Digitální podpis může vytvořit

a) Pouze osoba vlastnící veřejný klíč
b) Pouze osoba vlastnící soukromý klíč
c) Pouze osoba vlastnící certifikovaný klíč
d) Pouze osoba vlastnící sdílený klíč

B

14. V současných SIM (Subscriber Identity Module) kartách pro GSM sítě je uložen:

a) Statická aplikační data a veřejný certifikát operátora
b) Symetrický klíč
c) Asymetrický klíč
d) Statická aplikační data podepsána soukromým klíčem karty

B

15. Pro vztah řízení přístupu a autentizace platí:

a) řízení přístupu je obvyklou podmínkou pro autentizaci
b) autentizace je obvyklou podmínkou pro řízení přístupu
c) jde o ekvivalentní termíny
d) jedná se o dva naprosto nesouvisející pojmy

B

16. K prvkům hardwarové podpory řízení přístupu patří např.

a) randomizace adres haldy (heap), na kterých se alokují dynamické proměnné běžících programů
b) zákaz přístupu všem procesům kromě OS do adres paměti nižších než jistá hranice (tzv. fence address)
c) existence několika úrovní oprávnění (tzv. rings) definujících přístupnost různých registrů a strojových instrukcí
d) programovému kódu
e) tzv. zero address: pokud se proces pokusí přistupovat k nulové adrese, což bývá známkou chyby, je násilně zastaven
f) tzv. poštovní adresování: paměť je rozdělena na oblasti, aby OS mohl chránit paměť kontrolovou znalosti tajného PSČ (tzv. ZIP code)

BC

17. K čemu slouží MAC (Message authentication code)

a) K transformaci hašovací funkce
b) K ověření zprávy síťové karty
c) K zajištění integrity
d) K detekci chyb při přenosu dat
e) K zajištění důvěrnosti

CD

18. Určete existující politiky řízení přístupu:

a) biometrické řízení provozu
b) skryté řízení přístupu
c) volitelné řízení přístupu
d) nízkoúrovňové řízení přístupu
e) povinné řízení přístupu

CE

19. Mezi problémy při správě víceúrovňových systémů (MLS) typicky patří:

a) náročná administrace
b) nestabilita aplikací využívajících MLS
c) obtížná/nejednoznačná klasifikace dat
d) propojování jednotlivých MLS systémů
e) neexistující nástroje pro administraci
f) nevhodné chování procesů

ACD

20. Generátory passcode slouží pro

a) Urychlení generování sekvenčních čísel
b) Realizaci challenge-response (výzva-odpověď) protokolu
c) Bezpečné uložení dlouhodobých klíčů
d) Personalizaci elektronických pasů

BC

21. Které z výroků o autentizaci na základě rozpoznání obličeje nejsou pravdivé?

a) Autentizaci komplikuje změna účesu, náušnice a brýle.
b) Přesnost se v posledních 5 letech příliš nezlepšila.
c) Jedná se o velice výpočetně náročnou metodu autentizace.
d) Autentizaci komplikuje osvětlení a pozadí.

B

22. Český elektronický pas s aktivní autentizací:

a) Lze naklonovat snadno, pokud známe data z MRZ
b) Lze naklonovat jen pokud spolupracuje skutečný držitel pasu a zná svůj PIN
c) Nelze snadno naklonovat (vyžaduje získání soukromého klíče pasu, který nelze z pasu vyčíst) a proto klonovaní českého pasu zatím nebylo veřejně předvedeno.

C

23. Zaručený elektronický podpis

a) Je jednoznačně spojen s podepisující osobou
b) Autorizuje podepisující osobu ve vztahu k datové zprávě
c) Je spojen s dostatečnou finanční zárukou
d) Umožňuje detekci změn ve zprávě, ke které je připojen
e) Je jednoznačně ověřitelný
f) Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě

ADEF

24. Jaká primární autentizační metoda slouží k automatizované verifikaci identity předkladatele pasu?

a) Znalost tajemství ověřená pomocí protokolu výzva-odpověď
b) Biometriky (obličej, otisk prstu, duhovka...)
c) V čipu zakódovaný 128bitový identifikátor (platný typicky 10 let)
d) Znalost tajemství (v tomto případě PINu) zakódovaného v MRZ

B

25. Které biometrické charakteristiky bývají nazývány také dynamickými?

a) Fenotypické
b) genotypické
c) fyziologické
d) behaviorální

D

26. Pro ověření japonského elektronického pasu na českých hranicích je třeba:

a) CSCA certifikát Japonska, který je třeba předem získat diplomatickými prostředky
b) DS certifikát, který je možné vyčíst z pasu
c) CSCA certifikát Japonska, který si držitel pasu může přinést na CD nebo USB flash disku
d) CSCA certifikát ČR, který je třeba předem získat diplomatickými prostředky
e) CSCA certifikát Japonska, který je možné vyčíst z pasu
f) DS certifikát, který který si držitel pasu musí přinést na CD nebo USB flash disku

AB

27. Mezi obecné výhody tokenů nepatří:

a) Snadné zjištění ztráty.
b) Obtížná kopírovatelnost.
c) Možnost zpracovávání informací.
d) Snadná detekce a odpověď na narušení.

D

28. Ukládání hesel lze realizovat

a) Hlasovaně
b) Šifrovaně
c) Kryptovaně
d) V otevřené podobě
e) Hašovaně

BDE

29. Které časově proměnné parametry se používají v kryptografických protokolech?

a) Náhodná čísla
b) Monoliticky rostoucí sekvence
c) Časová razítka
d) Náhodná časová razítka
e) Náhodné sekvence
f) Náhodná komplexní čísla

AC

30. **Odpovědí na narušení se u čipových karet myslí:**

a) Po úspěšném provedení narušení jsou stopy narušení odstraněny.
b) Vlastnost části systému umožňující detekovat fyzický útok.
c) Akce provedená bezpečnostním administrátorem po zjištění pokusu o narušení.
d) Automatická akce provedená chráněnou částí při detekci pokusu o narušení.

D

31. Proces použití biometrik pro autentizaci zahrnuje

a) degustaci
b) verifikaci
c) registraci
d) demonstraci

BC

32. Slabá bezkoliznost u hašovacích funkcí znamená

a) V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)!=h(y)
b) Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že x=h(y)
c) Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=h(y)
d) Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=y

C

33. Běžné komerční biometrické zařízení

a) se neautentizuje vůči dalším komunikujícím.
b) je vybaveno detekcí průniku nebo má zvýšenou odolnost proti průniku.
c) typicky dobře šifruje přenášená data pomocí kvalitních algoritmů.

A

34. Pravděpodobnost, že se nepoctivý útočník může úspěšně vydávat za jinou stranu je u zero-knowledge protokolů (protokoly s nulovým rozšířením znalostí) mizivá. Tato vlastnost se nazývá:

a) Částečné uspokojení (partial satisfaction)
b) Úplné uspokojení (complete satisfaction)
c) Úplnost (completeness)
d) Korektnost (soundness)

D

35. Které z uvedených možností jsou proveditelnými útoky při provedení autentizace prostřednictvím .rhosts

a) Útok hrubou silou.
b) Vrácení podvržené IP adresy po dotazu na DNS server.
c) Uvedení nepředpokládaného loginu uživatele.
d) IP spoofing.

BCD

36. Vhodná tajná informace pro autentizaci je

a) Heslo
b) Fráze (passphrase)
c) Tel. číslo, pokud není uvedeno ve Zlatých stránkách
d) Rodné příjmení matky
e) PIN

ABE

37. Při používání digitálního podpisu používáme

a) Digitální klíč
b) Digitální pečetě
c) Privátní a veřejný klíč
d) Sdílené symetrické klíče mezi všemi komunikujícími partnery

C

38. Digitálně podepisujeme

a) V případě malých dokumentů celou zprávu, v případě velkých dokumentů jejich haš
b) Pouze haš podepisovaného dokumentu
c) Vždy přímo celý dokument

B

39. Matice přístupových práv

a) je reprezentace standardních přístupových práv v unixových OS (RWX-RWX-RWX)
b) zaznamenává pro každý objekt a každý subjekt údaje o čase, trvání, ... přístupu daného subjektu k danému objektu
c) má alespoň dva rozměry - subjekt a objekt
d) může mít i tři rozměry - subjekt, objekt a uživatel
e) definuje přinejmenším to, jaká přístupová práva mají jednotlivé subjekty k jednotlivým objektům

CE

40. Co je to odpověď na narušení?

a) Reakce chráněné části systému na probíhající pokus o útok.
b) Žádná z výše uvedených odpovědí.
c) Reakce nechráněné části systému na potencionální útok.
d) Služba internetového bankovnictví umožňující automaticky detekovat a upozornit na aktivní nebezpečný software v počítači.

A

41. Mezi reálně používané biometrické technologie patří

a) dynamika pohybu hlavy
b) vzor oční panenky
c) srovnání obličeje
d) otisk prstu
e) geometrie (tvaru) nohy

CD

42. Autentizace dat znamená

a) Potvrzení, že data nebyla neautorizovaně změněna od doby vytvoření
b) Data nemohl odeslat nikdo jiný než jejich původce
c) Potvrzení, že data pochází od určitého subjektu
d) Totéž co integrita

AC

43. Mezi základní nedostatky při snímání obličeje nepatří

a) zavřené oči.
b) nasazené kontaktní čočky.
c) nasazená čepice.
d) pestré a barevné pozadí.

B

44. Která z následujících tvrzení jsou platná pro protokol SSL/TLS?

a) Po průběhu Handshake protokolu je komunikace šifrována symetrickým klíčem.
b) SSL/TLS protokol zajišťuje integritu a autenticitu dat.
c) Autentizace komunikujících stran je založena na symetrické kryptografii.
d) Po úvodní Handshake protokolu je komunikace šifrována veřejným klíčem příjemce.

AB

45. Jaké vlastnosti mají magneto-optické čipové karty?

a) Poskytují magneto-optické rozhraní pro vysokorychlostní a prokazatelně bezpečný přenos dat.
b) Žádná z výše uvedených odpovědí.
c) Umožňují snímání čárových kódů zobrazovaných na monitoru při vstupu do internetového bankovnictví a jejich okamžité zpracování v čipu.
d) Neumožňují provádění kryptografických operací i přesto, že obsahují sofistikovanější magneto-optický proužek.

B

46. Jaké jsou používané algoritmy při digitálním podepisování

a) AES
b) RSA
c) El-Gamal
d) CBC
e) DSA

BCE

47. Která z tvrzení jsou platná pro termín "separace oprávnění" při řízení přístupu

a) tento termín neexistuje
b) týká se rozlišení procesů autentizace a autorizace
c) označuje stav, kdy je k provedení operace nutný souhlas více osob
d) žádní dva uživatelé systému nesmějí mít nikdy stejná oprávnění
e) vyjadřuje skutečnost, že se jednotlivé úrovně oprávnění nesmí překrývat

C

48. Co je vyžadováno pro autentizaci transakce při offline verifikaci se šifrováním PINu?

a) Originální PIN nutný pro verifikaci, který musí být bezpečně uložen v čipu
b) Úspěšné proběhnutí automatické správy rizik
c) Nový RSA pár klíčů pro šifrování PINů
d) Fyzicky i prostředím dobře zabezpečený PINpad

ACD

49. Pravděpodobnost, že se nepoctivý útočník může úspěšně vydávat za jinou stranu je u zero-knowledge protokolů (protokoly s nulovým rozšířením znalostí) mizivá. Tato vlastnost se nazývá:

a) Částečné uspokojení (partial satisfaction)
b) Korektnost (soundness)
c) Úplné uspokojení (complete satisfaction)
d) Úplnost (completeness)

B

50. Jaké kryptografické techniky lze využít pro implementaci autentizace čipu (jako součást EAC) u elektronických pasů?

a) Diffie-Hellman
b) SHA-1 a DSA
c) PGP
d) Fiat-Shamir
e) SHA-1 a 3DES
f) SHA-2 a AES

A

Viac som ich už nezohnal. :) Odpovede sú na 100% dobre. Prajem veľa šťasťia při skúške.