1. Aktualizace klíče se vzájemnou autentizací protokolem AKEP2 (Authenticated Key Exchange Protocol 2) je založena na:
   - [x] Algoritmu MAC (Message Authentication Code)
   - [ ] Generátorech passcode
   - [ ] Bezklíčových kryptografických hašovacích funkcích
   - [ ] Digitálních podpisech

---

2. Detekcí narušení se u čipových karet myslí:
   - [x] Vlastnost části systému umožňující detekovat fyzický útok.
   - [ ] Po narušení jsou stopy narušení obtížně odstranitelné.
   - [ ] Při zjištění narušení je automaticky provedena chráněnou části obranná akce.
   - [ ] Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.

---

3. Jednosměrnost u kryptografických hašovacích funkcí znamená
   - [ ] Pro dané h(y) nelze v rozumném čase najít x tak, aby h(x)=h(y)
   - [ ] V rozumném čase nejsme schopni najít x, y tak, aby h(x)=h(y)
   - [x] Pro dané y nelze v rozumném čase najít x tak, aby h(x)=y
   - [ ] Pro dané y lze v rozumném čase najít x tak, aby h(x)=y

---

4. Které z uvedených typů autentizačních kalkulátorů se používají v IT bezpečnosti?
   - [x] Kalkulátor s tajnou informací.
   - [x] Kalkulátor s hodinami.
   - [ ] Kalkulátor s vestavěným budíkem (z angl. embedded alarm).
   - [x] Kalkulátor bez vstupní klávesnice.

---

5. Při hašování hesel pro autentizaci uživatelů pomocí hesel:
   - [x] Při ukládání můžeme využít techniky "solení"
   - [ ] Ukládáme pouze haš hesla s možností rekonstrukce hesla v otevřené podobě
   - [x] Ukládáme pouze haš hesla a rekonstrukce otevřené podoby není možná

---

6. K čemu se používá CAPTCHA
   - [ ] K testu uživatelů, zda chtějí luštit text v obrázku a opisovat jej
   - [ ] Je to dynamicky se měnící designový prvek www stránek
   - [ ] K odlišení chytrých robotů od robotů první generace
   - [x] K odlišení uživatelů od robotů

7. PIN je

- [ ] Kombinace čísel a písmen (A-F) pro potřeby autentizace
- [x] Kombinace čísel pro potřeby autentizace
- [ ] Osobně sdílená informace
- [ ] Veřejně známá informace

8. Soubor /etc/passwd může obsahovat

- [ ] Informaci o délce hesla
- [x] Informaci o tom, že haše hesel jsou v souboru /etc/shadow
- [ ] Datum a čas posledního úspěšného přihlášení do systému
- [ ] Počet zbývajících neúspěšných pokusů o zadání hesla
- [x] Haše hesel uživatelů

9. Jaké jsou obecné výhody tokenů?

- [x] Rychlé zjištění ztráty.
- [ ] Nikdy je nelze zneužít po náhodném nálezu.
- [x] Většinou nejsou jednoduše kopírovatelné.
- [x] Mohou zpracovávat a přenášet další informace.

10. Jaké vlastnosti mají magneto-optické čipové karty?

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

11. V dobrých autentizačních protokolech se typicky

- [ ] Heslo posílá v otevřené podobě
- [x] Heslo neposílá vůbec
- [x] Heslo posílá v hašované podobě

12. Soubor /etc/shadow obsahuje

- [x] Haše hesel uživatelů
- [ ] Počet neúspěšných pokusů o zadání hesla
- [ ] Datum a čas posledního úspěšného přihlášení do systému
- [ ] Informaci o délce hesla
- [ ] Informaci o tom, že haše hesel jsou v souboru /etc/passwd

---

13. Jaká je správná sekvence operací při ověřování PINu odolná proti přerušení napájení?

- [ ] Test čítače pokusů větší než 0, zvýšení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- [ ] Test čítače pokusů větší než 0, ověření korektnosti PINu, snížení čítače při špatném PINu.
- [x] Test čítače pokusů větší než 0, snížení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- [ ] Zvýšení čítače, test čítače pokusů větší než 0, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.

---

14. Útok na hesla může být

- [x] Hrubou silou
- [ ] Matrixovou metodou
- [x] Na základě určitých znalostí o uživateli
- [x] Slovníkový
- [x] Pomocí sociálního inženýrství

---

15. K čemu slouží soubor .rhosts?

- [ ] Uchování informací o adresách autentizovaných počítačů připojených k serveru.
- [ ] K uchování RSA klíče(ů) serveru.
- [ ] K uchování uživatelů s právem číst (read).
- [x] K nastavení adres počítačů s povoleným přihlášením bez další autentizace .

---

16. V tiketu používaném v systému Kerberos se objevuje:

- [ ] Soukromý klíč
- [ ] Náhodná výzva
- [x] Časové razítko
- [x] Identifikátor alespoň jedné ze stran

---

17. Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) umožňují, poctivým stranám vždy dosáhnout úspěšného výsledku. Tato vlastnost se nazývá:

- [ ] Korektnost (soundness)
- [ ] Úplné uspokojení (complete satisfaction)
- [ ] Částečné uspokojení (partial satisfaction)
- [x] Úplnost (completeness)

---

18. K čemu slouží autentizační agent u ssh?

- [x] Opakované požadavky vyžadující heslo řeší agent po prvním zadání automaticky.
- [ ] Automaticky autentizuje server vůči uživateli bez nutnosti zadávat opakovaně heslo.
- [ ] K autentizaci dat přenášených mezi serverem a uživatelem.
- [ ] Autentizační agent se u ssh nepoužívá, neboť je použita asymetrická kryptografie.

---

19. Co nezajišťuje protokol ssh?

- [x] Ochranu proti analýze provozu.
- [x] Ochranu proti distribuovanému odmítnutí služby.
- [ ] Autentizaci uživatele.
- [ ] Autentizaci serveru.

---

20. Které z uvedených útoků na čipové karty nepatří mezi logické útoky?

- [ ] Časová analýza
- [ ] Útok přes aplikační rozhraní
- [x] Preparace čipu
- [x] Ozařování čipu

---

21. Útok na čipové karty pomocí časové analýzy využívá:

- [ ] Závislost průběhu odběru proudu na prováděné instrukci.
- [x] Délka operace v závislosti na zpracovávaných datech.
- [x] Délka operace v závislosti na vykonané větvi kódu.
- [ ] Závislost průběhu odběru proudu na zpracovávaných datech.

---

22. Co je to zaručený elektronický podpis

- [ ] Elektronický podpis, za který se dokážeme nějak důvěryhodně zaručit
- [x] Podpis vytořený pomocí kryptografických prostředků
- [ ] Podpis, který má záruky srovnatelné jako elektronický podpis
- [x] Jednoznačně ověřitelný podpis

---

23. Které z níže uvedených typů protokolů existují?

- [x] Protokoly pro ustavení klíče
- [x] Autentizační protokoly bez ustavení klíče
- [x] Neautentizované protokoly pro ustavení klíče
- [x] Autentizované protokoly pro ustavení klíče
- [ ] Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) pro ustavení klíče.

---

24. Které z uvedených možností nezajišťuje protokol IPsec?

- [ ] Integrita a autentizace původu dat.
- [x] Nepopiratelnost přijetí dat.
- [x] Ochranu proti analýze šifrovaného provozu na síťové vrstvě.
- [ ] Důvěrnost dat, ochrana proti přehrání.

---

25. Na jakém problému je založena bezpečnost RSA

- [x] Faktorizace čísel
- [ ] Eliptické křivky
- [ ] Obchodní cestující
- [ ] Diskrétní logaritmus

---

26. Co znamená pojem elektronický podpis ve smyslu zákona o elektronickém podpisu?

- [ ] Takový pojem zákon neobsahuje
- [ ] Ručně psaný podpis
- [x] Libovolná identifikující informace připojená ke zprávě
- [ ] To stejné, co digitální podpis

---

27. Proč je u tokenů založených na hodinách potřeba řešit otázku posuvu hodin?

- [ ] Žádná z výše uvedených odpovědí.
- [x] Nutnost synchronizace drobných odchylek mezi serverem a tokenem.
- [ ] Pravým důvodem je přechod na letní/zimní čas a přestupné roky.

28. Pro autentizaci obrazovou informací platí

- [ ] Uživatel musí správně vybarvit předložený obrázek
- [ ] Uživatel musí systému slovně popsat obrázek sloužící k autentizaci
- [x] Uživatel musí vybrat správný obrázek nebo jeho část
- [ ] Uživatel musí do systému nahrát správný obrázek

---

29. Útok na čipové karty pomocí odběrové analýzy využívá:

- [x] Závislost průběhu odběru proudu na prováděné instrukci.
- [x] Závislost průběhu odběru proudu na ukládaných datech do paměti EEPROM.
- [x] Závislost průběhu odběru proudu na zpracovávaných datech.
- [ ] Data získaná odběrem vzorku paměti EEPROM.

---

30. Jak zajistíme integritu veřejného klíče

- [ ] Utajením soukromé části veřejného klíče
- [ ] Pomocí párového privátního klíče
- [ ] Částečným utajením veřejného klíče
- [ ] Pomocí klíčované hašovací funkce
- [x] Pomocí certifikátu veřejného klíče

---

31. Které z uvedených režimů podporuje IPsec:

- [ ] Dynamický virtuální režim.
- [x] Transportní režim.
- [x] Tunelovací režim.
- [ ] Překladový režim.

---

32. Která tvrzení platí pro elektronickou značku

- [x] Technologicky jde o totéž co zaručený elektronický podpis
- [ ] Ověření elektronické značky je obtížnější než ověření elektronického podpisu
- [x] Elektronická značka je ke zprávě připojena tak, že je možné detekovat následné změny ve zprávě
- [x] Elektronické značky jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu

---

33. Odpovědí na narušení se u čipových karet myslí:

- [ ] Akce provedená bezpečnostním administrátorem po zjištění pokusu o narušení.
- [ ] Vlastnost části systému umožňující detekovat fyzický útok.
- [x] Automatická akce provedená chráněnou částí při detekci pokusu o narušení.
- [ ] Po úspěšném provedení narušení jsou stopy narušení odstraněny.

---

34. Pokud ukládáme hesla šifrovaně

- [ ] Nesmí být použit šifrovací algoritmus DSA
- [x] Šifrovací klíč musí být přístupný autentizační službě
- [x] Musíme věřit administrátorovi
- [ ] Musíme znát (jako uživatelé) šifrovací klíč

---

35. IP spoofing označuje:

- [ ] Zachycení IP odesílatele.
- [x] Podvržení IP adresy odesílatele.
- [ ] Podvržení IP adresy příjemce.
- [ ] Zachycení IP adresy odesílatele i příjemce.

---

36. Jaké jsou typické velikosti pamětí u současných čipových karet?

- [ ] < 100KB RAM, < 100KB ROM, > 1MB EEPROM
- [x] < 10KB RAM, ~100KB ROM, < 100KB EEPROM
- [ ] ~128KB RAM, ~512KB ROM, ~512KB EEPROM
- [ ] > 256KB RAM, ~100KB ROM, < 100KB EEPROM

---

37. Při používání digitálního podpisu používáme

- [x] Privátní a veřejný klíč
- [ ] Digitální klíč
- [ ] Sdílené symetrické klíče mezi všemi komunikujícími partnery
- [ ] Digitální pečetě

---

38. Jaké jsou možnosti prevence padělání tokenů?

- [ ] Čestné prohlášení všech uživatelů systému.
- [x] Kontrola a licence souvisejících živností.
- [x] Utajení některých informací nutných ke konstrukci tokenu.
- [x] Omezení dostupnosti potřebného vybavení.

- [x] Modifikace dostupného vybavení (modifikace vybraných barev u kopírky, vkládání identifikátoru).
- [ ] Utajení všech informací nutných ke konstrukci tokenu.

---

39. Na jakém druhu kryptografie je založena základní verze Kerbera?
    - [x] Symetrická
    - [ ] Asymetrická
    - [ ] Hybridní

---

40. Která z následujících tvrzení jsou platná pro protokol SSL/TLS?
    - [x] SSL/TLS protokol zajišťuje integritu a autenticitu dat.
    - [ ] Po úvodní Handshake protokolu je komunikace šifrována veřejným klíčem příjemce.
    - [x] Po průběhu Handshake protokolu je komunikace šifrována symetrickým klíčem.
    - [ ] Autentizace komunikujících stran je založena na symetrické kryptografii.

---

41. Jaké jsou obecné nevýhody tokenů?
    - [x] Bez tokenu není autorizovaný uživatel rozpoznán.
    - [ ] Cena tokenů je příliš vysoká pro komerční využití.
    - [ ] Ztráta tokenu vede většinou ke kompromitaci celého systému.
    - [x] Ke kontrole je obvykle třeba speciální čtečka nebo vycvičená osoba.

---

42. Která z uvedených tvrzení pro Encapsulated Security Payload (ESP) nejsou pravdivá?
    - [x] ESP zajišťuje integritu, autenticitu a důvěrnost dat, nezajišťuje však obranu proti útoku přehráním.
    - [x] ESP nemá zajištěnu integritu a autenticitu dat, zajišťuje pouze důvěrnost dat.
    - [x] ESP zajišťuje obranu proti analýze šifrovaného provozu na úrovni síťové vrstvy.
    - [ ] ESP zajišťuje integritu, autenticitu a důvěrnost dat.

---

43. Současné čipové karty:
    - [ ] Neumožňují provádění kryptografických operací.
    - [x] Umožňují provádění kryptografických operací symetrické a asymetrické kryptografie s využitím koprocesoru.
    - [ ] Umožňují pouze provádění kryptografických operací symetrické kryptografie.
    - [ ] Umožňují pouze provádění kryptografických operací asymetrické kryptografie.

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

- [ ] Náhodné sekvence
- [ ] Náhodná komplexní čísla
- [ ] Monoliticky rostoucí sekvence
- [x] Náhodná čísla
- [ ] Náhodná časová razítka
- [x] Časová razítka

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

- [x] Implicitně je autentizace serveru povinná, autentizace klienta je volitelná.
- [ ] Implicitně je autentizace serveru a klienta povinná.
- [x] SSL/TLS protokol neprovádí elektronické podepisování dat.
- [ ] Implicitně je autentizace serveru i klienta vypnuta.

46. Jaké jsou nevýhody autentizace hašovaným heslem?

- [x] Útok přehráním
- [ ] Náchylnost ke slovníkovému útoku
- [ ] Příliš snadná transformace na zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- [ ] Možnost impersonace

47. Proti jakým útokům brání protokol ssh?

- [ ] Odposlech hesla a pozdější přehrání (na uživatelově PC)
- [ ] Analýza šifrovaného provozu na síťové vrstvě
- [x] DNS/IP/Routing spoofing
- [x] Odposlech hesla a pozdější přehrání (na síťové vrstvě)

48. Co je to Chaffing and winnowing

- [x] "Oddělení zrna od plev"
- [x] Pro každý bit zprávy vytvoříme dvě zprávy (správný, chybný MAC), příjemce si ponechá zprávu se správným MAC
- [ ] Zprávu rozdělíme na jednotlivé bity a ty šifrujeme z využitím MAC každý zvlášť
- [ ] Každý bit zprávy zkopírujeme několikrát za sebe, aby se předešlo chybám v důsledku chybovosti MAC komunikačního kanálu

49. Která z uvedených tvrzení o uživatelově PINu jsou pravdivá (při standardním nastavení karty)?

- [x] Při změně zablokovaného PINu je třeba zadat odblokovací PIN a nový uživatelský PIN.
- [ ] Při změně zablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- [x] Při změně nezablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- [ ] Při změně nezablokovaného PINu stačí zadat nový uživatelský PIN.

---

50. K čemu slouží CRC (Cyclic redundancy check)

- [ ] K ověření autenticity dat
- [ ] Ke kompresi dat
- [x] K detekci chyb při přenosu dat
- [ ] K zašifrování dat

---

51. Které z uvedených útoků na čipové karty nepatří mezi fyzické útoky?

- [ ] Ozařování čipu
- [x] Časová analýza
- [x] Odběrová analýza
- [ ] Preparace čipu

---

52. Při kombinaci šifrování veřejným klíčem a podpisu dokumentu se doporučuje operace provést v následujícím pořadí:

- [x] Podpis, šifrování
- [ ] Šifrování, podpis
- [ ] Podpis, šifrování, podpis
- [ ] Na pořadí operací nezáleží
- [ ] Šifrování, podpis, šifrování

---

53. Co je to odpověď na narušení?

- [x] Reakce chráněné části systému na probíhající pokus o útok.
- [ ] Reakce nechráněné části systému na potencionální útok.
- [ ] Služba internetového bankovnictví umožňující automaticky detekovat a upozornit na aktivní nebezpečný software v počítači.
- [ ] Žádná z výše uvedených odpovědí.

---

54. Z jakých šifrovacích algoritmů se obvykle tvoří hašovací funkce?

- [ ] Proudová symetrická šifra
- [ ] Asymetrická šifra
- [ ] Hašovací funkci nelze vytvořit z žádného šifrovacího algoritmu
- [x] Bloková symetrická šifra

---

55. Která z uvedených tvrzení o tokenech založených na hodinách jsou pravdivá:

- [ ] Přístup k využití tokenu s hodinami musí být vždy chráněn PINem.
- [x] Je potřeba řešit otázku synchronizace hodin mezi serverem a tokenem.
- [x] Autentizační hodnota je vygenerována na základě aktuálního času a tajné informace.
- [ ] Token s hodinami nelze použít bez přítomnosti klávesnice.

---

56. Zajistit autentizaci digitálních dat a zpráv lze

- [x] Pomocí zaručeného elektronického podpisu
- [ ] Pomocí MAC
- [ ] Pomocí parciálně zaručeného elektronického podpisu
- [ ] Pomocí klasického (ručního) podpisu
- [ ] Pomocí klíčované hašovací funkce

---

57. Které z uvedených režimů nepodporuje IPsec:

- [ ] Transportní režim.
- [ ] Tunelovací režim.
- [x] Dynamický virtuální režim.
- [x] Překladový režim.

---

58. Jaká je nevýhoda digitálního podepisování prováděného až po zašifrování dat

- [ ] Výrazné urychlení kryptoanalýzy
- [x] Možnost snadného odstranění digitálního podpisu
- [ ] Žádná, naopak výhodou je možnost snadné verifikace podpisu ještě před dešifrováním
- [ ] Žádná, naopak, výhodou je možnost několikanásobného podepsání zašifrovaných dat

---

59. Jaký mechanismus je použit pro zajištění bezpečnosti v autentizační hlavičce IPsec?

- [ ] Message Authentication Code s náhodným číslem.
- [x] Message Authentication Code se sekvenčním číslem.

- [ ] Diffie-Hellman autentizace bez klíčů.
- [ ] Digitální podpis využívající RSA nebo DSA.

---

60. Které z uvedených možností autentizace klienta vůči serveru podporuje protokol ssh?
    - [x] RSA autentizaci klienta.
    - [ ] Využitím protokolu pro nulové rozšíření znalosti.
    - [x] Stroje uvedené v souborech .rhosts nebo hosts.equiv.
    - [ ] Heslem uživatele bez autentizace serveru.

---

61. Zaručený elektronický podpis
    - [ ] Autorizuje podepisující osobu ve vztahu k datové zprávě
    - [ ] Je spojen s dostatečnou finanční zárukou
    - [x] Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
    - [x] Je jednoznačně ověřitelný
    - [x] Umožňuje detekci změn ve zprávě, ke které je připojen
    - [x] Je jednoznačně spojen s podepisující osobou

---

62. 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:
    - [ ] Úplné uspokojení (complete satisfaction)
    - [x] Korektnost (soundness)
    - [ ] Úplnost (completeness)
    - [ ] Částečné uspokojení (partial satisfaction)

---

63. Úspěšnost útoku hrubou silou se dá odhadnout podle vzorce
    - [ ] (délka hesla * počet odhadů za jednotku času)/(velikost abecedy)^(čas platnosti)
    - [x] (čas platnosti * počet odhadů za jednotku času)/(velikost abecedy)^(délka hesla)
    - [ ] (počet odhadů za jednotku času * délka hesla)/(čas platnosti)^(velikost abecedy)
    - [ ] (velikost abecedy * délka hesla)/(počet odhadů za jednotku času)^(čas platnosti)

---

64. Při autentizaci tajnou informací je nutné dodržet

- [ ] Z tajné informace se musí nejprve vytvořit inicializační vektor
- [x] Prostor, ze kterého vybíráme hodnotu tajné informace musí být rozsáhlý
- [x] Tajnou informaci musí vědět jen oprávněný uživatel
- [ ] Tajnou informaci musíme sdělit administrátorovi pro případně admin. zásahy v našem systému

---

65. Útok na čipové karty přes aplikační rozhraní (API) je založen na:

- [x] Nezamýšleném dopadu zpracování útočníkem zaslaných specifických vstupních dat.
- [ ] Nedostupnosti aplikačního rozhraní vnitřnímu prostředí karty.
- [ ] Využití indukce chyb do zpracování dat zaslaných přes aplikační rozhraní.
- [x] Využití chyby v návrhu rozhraní.

---

66. Chybové hlášení o změně integritního součtu veřejného klíče serveru u SSH může být způsobeno

- [x] Podvržením serveru útočníkovým strojem
- [x] Změnou souboru s veřejným klíčem serveru na uživatelově PC
- [ ] Chybějícím záznamem veřejného klíče v souboru známých serverů
- [x] Změnou dlouhodobého klíče serveru jeho administrátorem

---

67. Které z uvedených typů karet se používají v IT bezpečnosti?

- [ ] Karty s bezkontaktním magnetickým proužkem.
- [x] Kontaktní karty s čipem.
- [x] Bezkontaktní karty s čipem.
- [x] SIM karty v mobilních telefonech.

---

68. Jaké typy záznamů lze používat na čipové kartě?

- [x] Lineární záznamy s pevnou nebo variabilní délkou.
- [ ] Exponenciální záznam s pevnou délkou.
- [x] Cyklické záznamy.
- [x] Nestrukturovaná data.

---

69. Ukládání hesel lze realizovat

- [x] V otevřené podobě
- [x] Hašovaně

- [ ] Hlasovaně
- [x] Šifrovaně
- [ ] Impulzně

---

70. Která z uvedených tvrzení o řízení přístupu k datům na čipových kartách jsou pravdivá?
    - [x] Každý soubor má přiřazenu hlavičku s přístupovými právy.
    - [x] Založeno především na řízení přístupu k souborům.
    - [ ] Data jsou uchována na magnetickém proužku a před použitím v čipu kontrolována.
    - [ ] Data na kartě nemohou být po zápisu nikdy čtena ani měněna.

---

71. Odolností vůči narušení se u čipových karet myslí:
    - [ ] Vlastnost části systému umožňující detekovat fyzický útok.
    - [ ] Ochrana proti útoku rušením radiového signálu (RFID).
    - [x] Vlastnost části systému chráněné proti neautorizované modifikaci podstatně lépe než zbylá část systému.
    - [ ] Automatická akce provedená chráněnou částí při zjištění pokusu o narušení.

---

72. Co je to hašovací funkce?
    - [ ] Funkce, která mapuje libovolně velký vstup na výstup s délkou 128, 192, 256 nebo 512 bitů
    - [x] Funkce, která mapuje libovolně velký vstup na výstup fixní délky a není prostá
    - [ ] Funkce, která mapuje libovolně velký vstup na výstup fixní délky a je prostá
    - [ ] Funkce, která mapuje vstup fixní délky na výstup variabilní délky (podle entropie vstupu)
    - [ ] Šifrovací funkce se schopností deprese vstupních dat

---

73. Z jakého důvodu se používá Server key namísto Host key pro vlastní autentizaci u SSH?
    - [ ] Zrychlení procesu autentizace serveru vůči klientovi.
    - [ ] Pro zajištění kompatibility s protokolem telnet.
    - [ ] Zrychlení procesu autentizace klienta vůči serveru.
    - [x] Ochrana dlouhodobého klíče Host key před kompromitováním.

---

74. Který z následujících protokolů je součásti SSL/TLS protokolu?

- [ ] IPSec protokol.
- [x] Handshake protokol.
- [ ] Kerberos protokol.
- [x] Record Layer protokol.

---

75. Přístupová hesla můžeme rozlišit na

- [x] Skupinová
- [x] Jednorázová
- [x] Unikátní pro danou osobu
- [ ] Původně neveřejná
- [ ] Jednocestná
- [ ] Veřejná

---

76. Jak eliminujeme útoky hrubou silou na PINy?:

- [ ] Pravidelnou změnou hodnoty PINu
- [ ] Školením uživatelů
- [x] Omezením počtu pokusů o zadání PINu

---

77. Slabá bezkoliznost u hašovacích funkcí znamená

- [ ] V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)!=h(y)
- [x] Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=h(y)
- [ ] Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že h(x)=y
- [ ] Pro dané x nejsme schopni v rozumném čase najít y!=x tak, že x=h(y)

---

78. Jaký je u ssh rozdíl mezi Server key a Host key?

- [ ] Server key je krátkodobý klíč použitý pro odvození Host key.
- [ ] Host key je krátkodobý klíč použitý pro vlastní autentizaci serveru.
- [x] Server key je krátkodobý klíč použitý pro vlastní autentizaci serveru.
- [x] Host key je dlouhodobý klíč.

---

79. Digitální podpis může vytvořit

- [x] Pouze osoba vlastnící soukromý klíč
- [ ] Pouze osoba vlastnící sdílený klíč
- [ ] Pouze osoba vlastnící veřejný klíč

- [ ] Pouze osoba vlastnící certifikovaný klíč

---

80. Digitálně podepisujeme
    - [ ] V případě malých dokumentů celou zprávu, v případě velkých dokumentů jejich haš
    - [x] Pouze haš podepisovaného dokumentu
    - [ ] Vždy přímo celý dokument

---

81. Které z uvedených možností jsou proveditelnými útoky při provedení autentizace prostřednictvím .rhosts
    - [x] Vrácení podvržené IP adresy po dotazu na DNS server.
    - [x] Uvedení nepředpokládaného loginu uživatele.
    - [x] IP spoofing.
    - [ ] Útok hrubou silou.

---

82. Integrita dat znamená
    - [ ] Data nebyla autorizovaně předána
    - [ ] Data nebyla neautorizovaně změněna pouze v průběhu přenosu nezabezpečeným kanálem
    - [ ] Data v původní podobě lze obnovit i přesto, že byla modifikována
    - [x] Data nebyla neautorizovaně změněna

---

83. Každá z dvou komunikujících stran má svůj symetrický klíč. Kolik zpráv se vymění ve Shamirově protokolu bez klíčů, aby obě strany sdílely stejný klíč?
    - [ ] žádná z těchto odpovědi není správná
    - [ ] 2
    - [x] 3
    - [ ] 4

---

84. Co je to narozeninový paradox?
    - [ ] Situace, kdy se začátkem roků rodí víc mužů než žen
    - [x] Lze jej ilustrovat faktem, že v sále s 23 lidmi je pravděpodobnost stejného data narození dvou lidí větší než 50 %
    - [ ] Pravděpodobnost nalezení stejného data narození k pevně zvolenému datu je při 23 lidech větší než 50 %
    - [x] Statisticky podložená vysoká úspěšnost nalezení kolize

---

85. Digitální podpis ověříme pomocí

- [x] Veřejného klíče podepisující osoby
- [ ] Soukromého klíče podepisující osoby
- [ ] Privátního klíče podepisující osoby
- [ ] Klíče sdíleného s podepisující osobou
- [x] Certifikátu veřejného klíče podepisující osoby

---

86. Které z následujících nejsou hašovací funkce

- [ ] MD4
- [ ] MD5
- [ ] SHA-1
- [x] RSA
- [x] RC4
- [x] AES

---

87. Co patří mezi bezpečnostní problémy používání bankovních karet s čipem?

- [ ] Špatná průkaznost nelegitimní autorizace platby pomocí PINu.
- [ ] Výpočetní výkon nepostačuje pro kryptografické zabezpečení transakcí.
- [x] Možnost odpozorování PINu na frekventovaných místech.
- [ ] Velká obtížnost kopírování karty.

---

88. Které časově konstantní parametry se používají v kryptografických protokolech?

- [ ] V omezeném čase monoliticky rostoucí sekvence (zabraňují tzv. borcení časové osy)
- [ ] Náhodná časová razítka (platná po určitou dobu - typicky několik desítek hodin)
- [ ] Komplexní čísla s fixní imaginární i reálnou složkou
- [ ] Sekvenční číslo (jeho hodnota závisí na implementaci)
- [x] Žádné z uvedených
- [ ] XOR hodnotou "-1" pro modifikaci náhodné výzvy (tzv. keksík)

---

89. Které z uvedených kategorií čipových karet podle technologie komunikace rozlišujeme?

- [ ] Hybridní karty.
- [x] Bezkontaktní karty.
- [ ] Polymorfní karty.
- [x] Konktaktní karty.

90. K čemu slouží MAC (Message authentication code)

- [ ] K ověření zprávy síťové karty
- [x] K detekci chyb při přenosu dat
- [ ] K transformaci hašovací funkce
- [x] K zajištění důvěrnosti
- [x] K zajištění integrity

91. Pro pojem výpočetní bezpečnost platí následující tvrzení.

- [ ] Ani jedno z uvedených tvrzení neplatí
- [x] Časová náročnost prolomení určitého algoritmu mnohonásobně převyšuje dostupný výpočetní výkon
- [x] Algoritmus jako takový nemusí být považován za neprolomitelný, dosud pouze nebyl nalezen efektivní způsob řešení/výpočtu
- [ ] Výsledek náročného výstupu je podepsaný, z důvodu zaručení integrity

92. Na jaké vrstvě funguje protokol SSL/TLS?

- [ ] na linkové vrstvě
- [ ] na síťové vrstvě
- [x] mezi aplikační a datovou vrstvou
- [ ] na datové vrstvě

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

- [ ] SSL/TLS protokol nezajišťuje důvěrnost dat.
- [ ] Implicitně je autentizace serveru a klienta je povinná.
- [x] SSL/TLS protokol umožňuje vzájemnou autentizaci serveru a klienta.
- [x] Autentizace komunikujících stran je založena na asymetrické kryptografii.

94. Které z uvedených odpovědí jsou pravdivé?

- [x] Cena výroby jednoho kusu tokenu klesá při výrobě mnohakusové série.
- [ ] Cena padělání jednoho kusu klesá při uplatnitelnosti mnohakusové série padělku.
- [ ] Cena padělání typicky nezávisí na počtu padělaných kusů.
- [ ] Relativní cena padělání se zvyšuje s každým dalším padělkem.

95. Protokol Kerberos zajišťuje

- [ ] Akumulaci
- [x] Autentizaci
- [ ] Autokracii
- [ ] Aprobaci

---

96. Útok na čipové karty pomocí indukce chyb je založen na:

- [x] Využití indukce chyb po prudkém ovlivnění vnějších podmínek k testování změny chování algoritmu.
- [x] Využití chybného běhu algoritmu po prudkém ovlivnění vnějších podmínek k získání tajných dat.
- [ ] Využití opravných kódů pro automatické odstranění chyby po prudkém ovlivnění vnějších podmínek.
- [ ] Jako první krok útoku je provedeno fyzického poškození.

---

97. Zjistitelností narušení se u čipových karet myslí:

- [x] Po narušení jsou stopy narušení obtížně odstranitelné.
- [ ] Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- [ ] Vlastnost části systému umožňující reagovat na fyzický útok.
- [ ] Při zjištění narušení je automaticky provedena chráněnou částí obranná akce.

---

98. Jaký je vztah mezi chybovou analýzou a útoky na a přes API?

- [ ] API mnohdy obsahuje četné chyby hodné důkladné analýzy.
- [ ] Chybová analýza je nezbytná součást každého útoku na a přes API.
- [ ] Každý útok na a přes API je nezbytnou součástí chybové analýzy.
- [x] Chybová analýza s útoky na a přes API nijak nesouvisí.

---

99. Které z uvedených možností zajišťuje protokol IPsec?

- [x] Důvěrnost dat, ochrana proti útoku přehráním.
- [x] Podporu správy klíčů.
- [ ] Nepopiratelnost přijetí dat.
- [x] Autentizace a integrita původu dat.

---

100. Fyzickou bezpečností se u čipových karet myslí:

- [ ] Ochrana proti fyzickému zkoušení PINu hrubou silou.

- [ ] Fyzická překážka kolem čipu karty ztěžující neutorizovaný přístup.
- [x] Odolnost proti útokům vyžadujícím fyzický přístup ke kartě.
- [ ] Ochrana proti hloubkové odběrové analýze na úrovni procesoru.

---

101. Které z uvedených kategorií čipových karet podle technologie uchování a práce s daty rozlišujeme?
- [x] Procesorové karty.
- [x] Paměťové karty se speciální logikou.
- [x] Paměťové karty.
- [ ] Karty s magnetickým proužkem.

---

102. Které protokoly umožňují vytvoření sdíleného tajemství?
- [ ] Silné autentizační protokoly
- [x] Protokoly pro ustavení klíče
- [ ] Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- [x] Protokoly implementované v Kerberu

---

103. Co zajišťujeme použitím náhodných čísel?
- [ ] Nezvratnost
- [x] Čerstvost
- [ ] Odolnost proti uváznutí a stárnutí
- [x] Aktuálnost
- [x] Jedinečnost
- [ ] Stálost a stabilitu

---

104. Co je to semi-invazivní časová analýza?
- [x] Žádná z výše uvedených odpovědí.
- [ ] Metrika sloužící k určení a vyhodnocení efektivnosti semi-invazivních útoků.
- [ ] Speciální semi-invazivní útok na autentizační kalkulátor s hodinami.
- [ ] Druh semi-invazivního útoku zneužívající u mnohých čipových karet možnost ovlivnění vstupního hodinového cyklu.

---

105. Protokoly výzva-odpověď mohou být založeny na:

- [x] symetrickém šifrování
- [x] MAC kódu, resp. funkci
- [x] klíčované hašovací funkci
- [x] digitálním podpisu

---

106. U autentizace pomocí hesel

- [x] Musíme řešit aspekt zapamatovatelnosti vs. bezpečnosti
- [ ] Musí uživatel prokázat, že si dokáže zapamatovat alespoň 10 náhodně zvolených symbolů
- [ ] Musíme řešit aspekt bezpečnosti bez ohledu na zapamatovatelnost

---

107. Čeho lze dosáhnout zopakováním zero-knowledge protokolu (protokol s nulovým rozšířením
znalostí)?

- [ ] Ničeho - nezvýší se záruka, že nedojde k rozšíření žádných znalostí
- [x] Zvýšení bezpečnosti - sníží se pravděpodobnost, že nepoctivý útočník se může úspěšně vydávat za jinou stranu
- [ ] Zvýšení bezpečnosti - zvýší se záruka, že nedojde k rozšíření žádných znalostí
- [ ] Ničeho - ke spolehlivé autentizaci stačí 1 kolo protokolu

---

108. Generátory passcode slouží pro

- [x] Realizaci challenge-response (výzva-odpověď) protokolu
- [x] Bezpečné uložení dlouhodobých klíčů
- [ ] Urychlení generování sekvenčních čísel
- [ ] Personalizaci elektronických pasů

---

109. Pro bezpečné používání digitálního podpisu

- [ ] Je nutné zajistit integritu parciálního klíče
- [x] Je nutné udržet privátní klíč v tajnosti
- [x] Je nutné zajistit integritu veřejného klíče
- [ ] Je nutné udržet veřejný klíč v tajnosti

---

110. Která z uvedených tvrzení jsou pravdivá:

- [ ] Autentizace pomocí IP adresy je výrazně bezpečnější než autentizace pomocí MAC adresy.

- [ ] Autentizace pomocí IP adresy může být použita pouze v kombinaci s MAC adresou.
- [x] Autentizace pomocí IP adresy není spolehlivá, protože IP může být změněna.
- [ ] Autentizace pomocí IP adresy je výrazně méně bezpečná než autentizace pomocí MAC adresy.

---

111. Které protokoly zaručují určitou míru jistoty o identitě jiné strany?
- [x] Autentizační protokoly
- [x] Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- [x] Protokoly implementované v Kerberu
- [ ] Protokoly pro ustavení klíče

---

112. Které z protokolů se v současnosti v běžných aplikacích využívají více?
- [ ] Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- [x] Challenge-response protokoly (protokoly výzva-odpověď)

---

113. Jaký typ pamětí je typicky používán u současných čipových karet?
- [ ] GRAM
- [ ] DRAM
- [x] SRAM
- [x] EEPROM

---

114. Jaké jsou používané algoritmy při digitálním podepisování
- [ ] CBC
- [x] El-Gamal
- [ ] AES
- [x] RSA
- [x] DSA

---

115. Co patří mezi bezpečnostní problémy používání bankovních karet pouze s magnetickým proužkem?
- [x] Přítomný hologram se obtížně automatizovaně kontroluje.
- [ ] Malá odolnost proti chybové analýze.
- [x] Relativně jednoduše se kopírují.
- [ ] Autentizační podpis je součástí karty.

---

116. Vhodná tajná informace pro autentizaci je

- [x] Fráze (passphrase)
- [x] PIN
- [x] Heslo
- [ ] Tel. číslo, pokud není uvedeno ve Zlatých stránkách
- [ ] Rodné příjmení matky

---

117. Mezi obecné výhody tokenů nepatří:

- [ ] Snadné zjištění ztráty.
- [ ] Obtížná kopírovatelnost.
- [x] Snadná detekce a odpověď na narušení.
- [x] Možnost zpracovávání informací.

---

118. Které z příkladů autentizace počítačů jsou možné:

- [x] Kombinace IP adresy a tajného klíče symetrické kryptografie.
- [x] Tajným klíčem symetrické kryptografie.
- [x] Kombinace IP, MAC, GUID (global unique identifier).
- [x] Privátním klíčem asymetrické kryptografie.

---

119. Co je to heslo založené na frázi?

- [ ] Heslo založené na veřejně známé frázi, aby si jej všichni snadno zapamatovali
- [ ] Heslo, které lze jednoduše přečíst
- [ ] Heslo, které obsahuje pouze malá písmena
- [x] Pomůcka pro zapamatování složitého hesla

---

120. Autentizace dat znamená

- [ ] Totéž co integrita
- [x] Potvrzení, že data nebyla neautorizovaně změněna od doby vytvoření
- [ ] Data nemohl odeslat nikdo jiný než jejich původce
- [x] Potvrzení, že data pochází od určitého subjektu

---

121. Jaké vlastnosti má Shamirův protokol bez klíčů (Shamir’s no-key protocol)

- [x] Vyžaduje komutativní šifrovací algoritmus
- [ ] Umožňuje vzájemnou autentizaci
- [ ] Prokazuje, že P!=NP

- [ ] Funguje obzvláště dobře (a prokazatelně bezpečně) jen při použití One-Time Pad
- [x] Nevyžaduje žádné ustavení sdílených klíčů

---

122. Která z uvedených tvrzení o autentizačních kalkulátorech jsou pravdivá?
- [x] Pracují na principu protokolu výzva/odpověď s využitím tajné informace.
- [x] Přístup k využití kalkulátoru může být chráněn PINem.
- [x] Výzva je zadávána manuálně nebo automaticky načtena z vhodného média.
- [ ] Kalkulátor nelze zneužít i při znalosti PINu.

---

123. "Solení" hesel
- [ ] Je dodatečná technika při ukládání hesel pro určitou formu identifikace
- [ ] Je dnes již jen velmi zřídka používaná technika
- [x] Zajistí delší efektivní heslo
- [x] Pomůže vyřešit situaci, kdy mají uživatelé stejná hesla

---

124. Silná bezkoliznost u hašovacích funkcí znamená
- [ ] V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)=h(y)
- [ ] V rozumném čase nejsme schopni nalézt x, y (x=y) tak, že h(x)!=h(y)
- [x] V rozumném čase nejsme schopni nalézt x, y (x!=y) tak, že h(x)=h(y)
- [ ] V rozumném čase nejsme schopni nalézt x, y (x!=y) tak, že h(x)!=h(y)