Started on	Tuesday, 24 May 2011, 04:03 PM
Completed on	Tuesday, 24 May 2011, 04:23 PM
Time taken	19 mins 44 secs
Grade	**13.7** out of a maximum of 25 (**55**%)

1

Marks: 1

Jak je u protokolu WPA zajištěna integrita přenášených dat proti úmyslným změnám?

Choose one answer.

- a. pomocí protokolu TKIP
- b. není zajištěna
- c. pomocí protkolu CHAP
- d. pomocí algoritmu CRC32
- e. pomocí algoritmu MIC
- f. pomocí protokolu EAP-TLS

Incorrect
Marks for this submission: 0/1.

2

Marks: 1

Prokázání totožnosti se odborně nazývá:

Choose one answer.

- a. šifrování
- b. šikana policejního státu
- c. nepopiratelnost
- d. autentizace
- e. autorizace
- f. biometrika

Correct
Marks for this submission: 1/1.

3

Marks: 1

Diffie-Hellmanův algoritmus lze použít k:

Choose one answer.

- a. výměně klíčů
- b. šifrování a podepisování
- c. podepisování
- d. šifrování
- e. šifrování, podepisování a výměně klíčů

Incorrect
Marks for this submission: 0/1.

4

Marks: 1

Šifrování s asymetrické kryptosystémy je v porovnání se symetrickými:

Choose one answer.

- a. srovnatelně rychlé
- b. přibližně dvakrát rychlejší
- c. přibližně 100x rychlejší
- d. přibližně 100x pomalejší
- e. Asymetrické a symetrické kryptosystémy nelze z tohoto hlediska srovnávat.
- f. přibližně dvakrát pomalejší

Incorrect
Marks for this submission: 0/1.

5

Marks: 1

Alice digitálně podepisuje zprávu pro Boba. Podpis provede:

Choose at least one answer.

- [ ] a. zašifrováním celé zprávy veřejným klíčem Boba
- [x] b. zašifrováním celé zprávy privátním klíčem Alice
- [ ] c. zašifrováním celé zprávy privátním klíčem Boba
- [ ] d. zašifrováním celé zprávy veřejným klíčem Alice
- [ ] e. zašifrováním otisku zprávy veřejným klíčem Alice
- [x] f. zašifrováním otisku zprávy privátním klíčem Alice

Partially correct
Marks for this submission: 0.8/1.

6

Marks: 1

Která tvrzení jsou pravdivá o protokolu CHAP:

Choose at least one answer.

- [ ] a. autentizaci zahajuje server
- [ ] b. autentizace může probíhat kdykoliv během spojení
- [ ] c. heslo se přenáší v otevřeném tvaru
- [ ] d. jedná se o protokol typu výzva-odpověď
- [x] e. autentizaci zahajuje klient
- [x] f. autentizace probíhá pouze na počátku spojení

Incorrect

Marks for this submission: 0/1.

7

Marks: 1

Operace SubBytes plní v algoritmu AES stejnou roli, jako blok <ZVOLTE> v algoritmu DES.

Choose one answer.

- ( ) a. K-box
- (•) b. S-box
- ( ) c. X-box
- ( ) d. E-box
- ( ) e. IN-box
- ( ) f. P-box

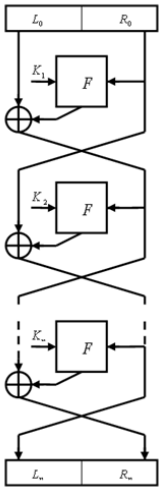
Correct

Marks for this submission: 1/1.

8

Marks: 1

Na obrázku je znázorněn



Choose one answer.

- (•) a. obecný tvar Feistelovy šifry
- ( ) b. model RSA
- ( ) c. model Diffie-Hellmanova algoritmu
- ( ) d. jedna runda algoritmu AES
- ( ) e. model elektronického podpisu
- ( ) f. model proudové šifry

Correct

Marks for this submission: 1/1.

9

Marks: 1

Které podmínky musí být splněny, aby Vernamova šifra byla absolutně bezpečným kryptostystémem ?

Choose at least one answer.

- [ ] a. klíč lze použít maximálně třikrát za rok
- [ ] b. klíč musí být být generován v certifikovaném SW na zabezpečeném počítači
- [ ] c. klíč musí být minimálně o polovinu kratší než délka OT
- [x] d. jiná správná odpověď
- [ ] e. klíč musí znát pouze odesílatel, příjemce a certifikační autoria

Correct

Marks for this submission: 1/1.

10

Marks: 1

Která operace v rámci jedné rundy je z hlediska bezpečnosti DESu nejdůležitější?

Choose one answer.

- ( ) a. dynamická permutace P-boxu
- ( ) b. expanzní permutace v E-boxu
- ( ) c. přičítání klíčů v K-boxu
- ( ) d. modulární umocňování v M-boxu
- ( ) e. prohazování polovin bloků mezi rundami
- (•) f. subtituce v S-boxu

Correct

Marks for this submission: 1/1.

11

Marks: 1

Při šifrované komunikaci s použitím symetrického algoritmu mezi N subjekty bez použití dalších technologií pro distribuci klíčů je potřeba <DOPLŇTE> různých klíčů:

Pozn.: předpokládejte, že pro komunikaci mezi dvojicí účastníků A,B (A->B a B->A) se použijí dva různé klíče

Choose one answer.

- ( ) a. N-1
- ( ) b. N(N-1)/2
- ( ) c. 2^(N-1)
- ( ) d. N(N+1)/2
- (•) e. N^2
- ( ) f. N(N-1)

Incorrect

12

Marks: 1

Odolnost vůči získání přelohy znamená, že:

Choose one answer.

- ( ) a. je výpočetně nemožné nalézt ke vstupu x druhý vstup x' takový, že x'≠ x a zároveň h(x')=h(x).
- ( ) b. je výpočetně nemožné systematicky vytvářet dva libovolné různé vstupní texty x a x' pro které platí, že x' ≠ x a zároveň h(x)=h(x')
- ( ) c. je obtížné nalézt x a y taková, že x≠y a zároveň H(x) a H(y) se liší jen v malém počtu bitů.
- (•) d. Nelze najít předobraz x' takový, že h(x')=y, když známe pouze h a y a neznáme x' .

Correct

Marks for this submission: 1/1.

13

Marks: 1

Informace o použitých kryptografických algorimtech a klíčích je u protokolu IPsec uchovávána v:

Choose one answer.

- ( ) a. SPD
- ( ) b. RLP
- ( ) c. SPI
- ( ) d. ESP
- ( ) e. SAD

Incorrect

Marks for this submission: 0/1.

14

Marks: 1

Protokol CCSP(Change Cipher Specification Protocol) má u TLS 1.0 na starosti:

Choose at least one answer.

- [ ] a. kompresi přenášených dat
- [ ] b. dojednání šifrovacích algoritmů
- [x] c. ohlášení změny používaných algoritmů a klíčů
- [ ] d. hlášení chyb
- [ ] e. šifrování přenášených dat
- [x] f. výměnu klíčů

Partially correct

Marks for this submission: 0.8/1.

15

Marks: 1

Délka výstupu hashovací funkce SHA-256 je <DOPLŇTE> bitů.

Answer: 228

Incorrect

Marks for this submission: 0/1.

16

Marks: 1

Nejstarší protokol pro zabezpeční bezdrátových sítí 802.11 se jmenuje <DOPLŇTE zkratku velkými písmeny>.

Answer: WEP

Correct

Marks for this submission: 1/1.

17

Marks: 1

Schopnost systému zajišťující, že přenášená informace nebyla zničena, ztracena nebo modifikována, resp. detekce takovéto změny se nazývá

Choose at least one answer.

- [ ] a. utajení
- [ ] b. nepopiratelnost
- [ ] c. autorizace
- [ ] d. autentizace
- [x] e. integrita
- [x] f. důvěryhodnost
- [ ] g. zabezpečení

Partially correct

Marks for this submission: 0.8/1.

18

Marks: 1

Certifikát standardu X.509v3 obsahuje

Choose at least one answer.

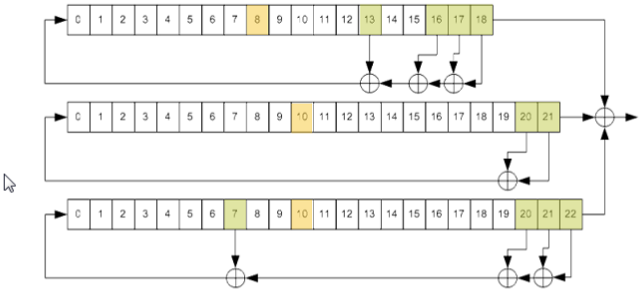
- [ ] a. privátní klíč certifikační autority
- [ ] b. privátní klíč majitele certifikátu
- [x] c. veřejný klíč certifikační autority
- [x] d. datum a čas platnosti certifikátu
- [ ] e. veřejný klíč majitele certifikátu
- [ ] f. ani jednu z uvedených položek neobsahuje

Partially correct

19

Marks: 1

Algoritmus znázorněný obrázku v každém kroku vygeneruje



Choose one answer.

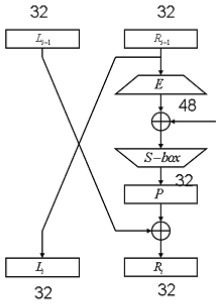
- ( ) a. 3 bity proudu klíče
- (•) b. 1 bit proudu klíče
- ( ) c. 2 bity proudu klíče
- ( ) d. 3 bajty proudu klíče
- ( ) e. 1 bajt proudu klíče
- ( ) f. 128 bitů proudu klíče

Correct

Marks for this submission: 1/1.

20 Marks: 1

Na obrázku je znázorněna vnitřní struktura jedné blokové šifry. O jaký algoritmus se jedná ?



Choose one answer.

- a. DES
- b. AES
- c. RC6
- d. RC4
- e. Serpent
- f. A5

Correct
Marks for this submission: 1/1.

21 Marks: 1

Elektronicky podepsat lze:

Choose one answer.

- a. libovolná digitální data
- b. pouze textové dokumenty ve formátu TXT
- c. pouze textové dokumenty ve formátu DOC
- d. pouze emaily bez přílohy (podle RFC 822)
- e. všechny dokumenty MS Office od verze 2007

Correct
Marks for this submission: 1/1.

22 Marks: 1

Protokol IKE zajišťuje:

Choose one answer.

- a. ochranu proti replay útokům
- b. výměnu klíčů pro protokoly AH a ESP
- c. autentizaci přenášených dat
- d. se dnes již nepoužívá
- e. šifrování uživatelských dat

Incorrect
Marks for this submission: 0/1.

23 Marks: 1

Výhodou režimu ECB je:

Choose at least one answer.

- [x] a. jednoduchá paralelizace dešifrování
- [ ] b. schopnost realizovat proudovou šifru
- [x] c. jednoduchá paralelizace šifrování
- [ ] d. odolnost proti cut-and-paste útoku
- [ ] e. závislost po sobě jdoucích bloků ŠT
- [ ] f. odolnost proti modifikaci bloku

Correct
Marks for this submission: 1/1.

24 Marks: 1

Kolik rund má algoritmus AES pro délku bloku i klíče 128 bitů?

Answer: 33

Incorrect
Marks for this submission: 0/1.

25

Marks: 1

Bezpečnost algoritmu DSA(Digital Signature Algorithm) je založena na obtížnosti řešení problému:

Choose one answer.

- a. NSA
- b. ECDH
- c. ECDLP
- d. RSA
- e. IFP
- f. DLP

Incorrect

Marks for this submission: 0/1.