Klausimai 2015 metų kriptografijos ir informacijos saugos kurso egzaminui

Skaitiniai klausimų duomenys egzamino užduotyje gali skirtis nuo šiame sąraše pateiktųjų. Vieno klausimo vertė – 1/2 balo.
Literatūros nuorodas rasite kurso tinklalapyje.
Sėkmės!

1. Įvadas

1.1. Kokius informacijos apsaugos uždavinius sprendžia kriptografija?
1.3. Suformuluokite kriptosistemos apibrėžimą?
1.3. Kas suformulavo moderniosios kriptografijos principus? Jei prisimenate bent vieną iš jų, tai suformuluokite?
1.4. Kokios kriptosistemos vadinamos simetrinėmis?
1.5. Paaiškinkite simetrinės kriptosistemos naudojimą diagrama.
1.6. Kokios kriptosistemos vadinamos nesimetrinėmis (viešojo rakto)?
1.7. Paaiškinkite simetrinės kriptosistemos naudojimą diagrama.
1.8. Paaiškinkite, kaip naudojamos skaitmeninių parašų schemos.
1.9. Kas yra pavienių šifrų ataka? Kas yra teksto-šifro porų ataka?
1.10. Kokia kriptosistema vadinama besąlygiškai saugia (unconditional security)?
1.11. Kokia kriptosistema vadinama saugia skaičiavimų požiūriu (computational security)?

3. Simetrinės kriptosistemos

3.1. Kas yra simbolių dažniai natūralioje kalboje ir kaip jie keičiasi, kai naudojame kriptosistemą su perstatomis?
3.3. Paaiškinkite, kaip veikia skytalės šifras.
3.3. Kas yra simbolių dažniai natūralioje kalboje ir kaip jie keičiasi, kai naudojame kriptosistemą su keitiniais?
3.4. Paaiškinkite, kaip konstruojamos kriptosistemos naudojantis Polibijaus kodo idėja.
3.5. Paaiškinkite Cezario kriptosistemą naudodami lyginius.
3.6. Cezario kriptosistemos abėcėlė $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6\}$. Šifras $c = \langle 3, 2, 4, 5\rangle$ gautas naudojant raktą $k = 3$. Dešifruokite šį šifrą.
3.7. Paaiškinkite, kaip veikia Hilo kriptosistema.
3.8. Hilo šifro abėcėlė $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6\}$. Užšifruokite simbolių porą $\langle 3, 5\rangle$ naudodami raktą

$$K = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$

3.9. Paaiškinkite Plaifairo šifrą.
3.10 Kas yra homofoniniai keitiniai ir kaip jie gali būti naudojami kriptosistemose?
3.11. Kaip keičiasi simbolių dažniai, kai naudojame homofoninius keitinius?

3. Vigenere kriptosistema, mechaniniai įrenginiai

3.1. Apibrėžkite Vigenere kriptosistemą naudodami lyginius.
3.2. Vigenere kriptosistemos abėcėlė $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6\}$. Užšifruokite pranešimą $P = 166166$ su raktu $k = 23$.
3.3. Vigenere kriptosistemos abėcėlė $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6\}$. Iššifruokite šifrą $C = 166166$, jeigu jis sudarytas panaudojus raktą $k = 23$.

3.4. Paaiškinkite, kaip galima analizuoti Vigenere kriptosistemą žinant rakto ilgį.
3.5. Paaiškinkite, kaip Vigenere šifro analizei galima taikyti Kassiskio testą.
3.6. Kas yra koincidencijų (sutapimų) indeksas?
3.7. Kaip taikomas kappa testas?
3.8. Paaiškinkite šifravimą su Jeffersono cilindrais.
3.9. Paaiškinkite šifravimo su rotorių įrengimais principą.
3.10. Teksto ir šifro abėcėlė yra $\mathcal{A} = \{0, 1, 2, 3, 4\}$, šifravimui naudojami du rotoriai, abiejų jungtys aprašomos tuo pačiu keitiniu $\lambda = [2, 0, 1, 4, 3]$. Kokia raide šifruojama raidė 0, jeigu ji yra tekste 12-oji? Šifravimą paaiškinkite.

4. Feistelio iteracijos, DES ir AES
4.2. Paaiškinkite brėžiniu šifravimo naudojant Feistelio iteracijas idėją.
4.3. Feistelio schemos funkcija $f(x_1x_2, y_1y_2) = z_1z_2$, čia $z_1 = x_1 \oplus y_1, z_2 = x_2y_3$. Kokį pranešimo 0111 šifrą gautume po dviejų iteracijų, jeigu abiejose naudojamas tas pats raktas $k = k_1k_2$ (išreikškite šifrą rakto bitais).
4.3. Kaip dešifruojamas šifras, gautas naudojant Feistelio iteracijas?
4.4. Nubraižykite vienos DES iteracijos schemą.
4.5. Kokio dydžio informacijos blokus šifruoja DES ir kokius raktus naudoja?
4.6. Paaiškinkite, kokie pranešimo bloko pertvarkiai sudaro vieną AES iteraciją.
4.7. Paaiškinkite, kaip DES buvo panaudota UNIX sistemoje autentifikavimui su slaptažodžiais.
4.8. Paaiškinkite blokinių kriptosistemų naudojimą CBC režimu.
4.9. Paaiškinkite blokinių kriptosistemų naudojimą OFB režimu.
4.10. Paaiškinkite blokinių kriptosistemų naudojimą CTR režimu.

5. Srautiniai šifrai
5.1. Nubraižykite kokią nors tiesinių registrų sistemos su trimis registrais schemą ir paaiškinkite kaip sistema generuoja rakto srautą.
5.2. Įrodykite, kad tiesinė registrų sistema generuoja periodinę bitų seką.
5.3. Kas yra registrų sistemos charakteringasis daugianaris ir kaip nuo jo savybių priklauso generuojamos sekos periodas?
5.4. Kaip atlikti kriptosistemos, kurioje naudojama registrų sistema, teksto-šifro poros ataką?
5.5. Paaiškinkite, kaip veikia šifras A5/1.
5.6. Paaiškinkite, kaip veikia šifras RC4.
5.7. Paaiškinkite, kaip galima jungti tiesinių registrų sistemas, kad būtų panaikinti tiesiniai rakto srauto bitų ryšiai.

6. h-funkcijos
6.1. Paaiškinkite, kas yra h-funkcija ir kam ji naudojama kriptografijoje?
6.2. Kas yra h-funkcijos sutapimas (kolizija)?
6.3. Kokios h-funkcijos vadinamos wcf ir scf h-funkcijomis?
6.4. Kas yra h-funkcijos „gimtadienių ” ataka?
6.5. Paaiškinkite Merkle-Damgaardo schemą maišos funkcijoms konstruoti.
6.6. Kaip maišos funkcijos gali būti konstruojamos naudojantis kriptosistemomis?
6.7. Paaiškinkite bendrais bruožais maišos funkcijos MD5 struktūrą.
6. 8. Paaiškinkite Keccac maišos funkcijos struktūrą.

7. Matematiniai viešojo rakto kriptografijos pagrindai

7.1. Paaiškinkite Euklido algoritmą skaičių bendrajam didžiausiam dalikliui rasti.

7.2. Užrašykite veiksmų, atliekamų ieškant skaičių 27 ir 15 bendrojo didžiausiojo daliklio Euklido algoritmu, lygybes.

7.3. Paaiškinkite kėlimo laipsniu duotuoju moduliu algoritmą.

7.4. Paaiškinkite kėlimo laipsniu duotuoju modulių algoritmą skaitiniu pavyzdžiu $7^{14} \bmod 5$.

7.5. Apibrėžkite Oilerio funkciją.

7.6. Suformuluokite Oilerio teoremą.

7.7. Apskaičiuokite $\phi(50)$.

7.8. Suformuluokite kiniškąją liekanų teoremą.

7.9. Pasinaudoję kiniškąja liekanų teorema suraskite skaičių x, tenkinantį lygybes
$x \equiv 2 \pmod 3, x \equiv 3 \pmod{17}$.

7.10. Kas yra elemento atvirkštinis moduliu n? Kokie elementai turi atvirkštinius?

7.12, Apskaičiuokite $3^{-1} \bmod 17$ pasinaudoję Euklido algoritmu.

8. RSA kriptosistema

8.1. Kaip sudaromi RSA kriptosistemos raktai?

8.2. Sudarykite RSA raktų porą su pirminiais $p = 5, q = 7$.

8.3. Kaip šifruojama ir dešifruojama RSA kriptosistemoje?

8.4. Įrodykite, kad RSA kriptosistemos dešifravimo algoritmas veikia teisingai.

8.5. Kuo remiasi RSA kriptosistemos saugumas?

8.6. Kaip RSA galima naudoti kaip skaitmeninio parašo schemą?

8.7. Paaiškinkite kaip atlikti RSA kriptosistemos vienodų modulių ataką.

9. „Kuprinės“ ir Rabino kriptosistemos

9.1. Suformuluokite kuprinės uždavinį.

9.2. Kokios svorių sistemos vadinamos sparčiai didėjančiomis?

9.3. Pateikite sparčiai didėjančios svorių sistemos pavyzdį.

9.4. Kaip spręsti kuprinės uždavinį, kai svorių sistema yra sparčiai didėjanti?

9.5. Išspręskite kuprinės uždavinį, kai svorių sistema $W = \{1, 3, 5, 12, 23, 45\}$, o svoris $m = 62$,

9.6. Kaip sudaromi Merkle ir Hellmano kuprinės kriptosistemos raktai?

9.7. Kaip šifruojama ir dešifruojama naudojantis Merkle ir Hellmano kuprinės kriptosistema?

9.8. Įrodykite, kad kuprinės kriptosistemos dešifravimo algoritmas veikia teisingai.

9.9. Apibrėžkite Rabino kriptosistemą.

9.10. Lyginio $x^2 \equiv 14 \pmod{43}$ sprendinys tikrai egzistuoja. Kaip galima jį greitai surasti?

9.11. Paaiškinkite, kaip dešifruojamas Rabino kriptosistemos šifras.

10. Diskretusis logaritmas ir jo taikymai

10.1. Kas yra generuojantis grupės $\mathbb{Z}_p$ elementas?

10.2. Kaip ieškoti grupės $\mathbb{Z}_p$ generuojančio elemento?

10.3. Patikrinkite, ar $g = 2$ yra $\mathbb{Z}_7$ generuojantis elementas.

10.4. Suraskite vieną $\mathbb{Z}_{11}$ generuojantį elementą. Užrašykite, kokius skaičiavimus atlikote.

10.5. Kas yra elemento $x \in \mathbb{Z}_p$ diskretusis logaritmas pagrindu g?

10.6. Kaip šifruojama ir dešifruojama ElGamalio kriptosistemoje?

10.7. Įrodykite, kad ElGamalio kriptosistemoje dešifravimo algoritmas veikia teisingai.

10.8. Kuo pagrįstas ElGamalio kriptosistemos saugumas?

10.9. Kaip sudaromas ElGamalio skaitmeninis parašas?
10.10. Paaiškinkite, kaip atlikti ElGamalio skaitmeninio parašo schemos ataką, turint du parašus, sudarytus su tuo pačiu parametru k.
10.11. Paaiškinkite Shankso algoritmą diskrečiajam logaritmui rasti.

11. Raktų nustatymo protokolai
11.1. Paaiškinkite Wide-Mouth Frog protokolą.
11.2. Paaiškinkite Needhamo-Schroederio raktų nustatymo protokolą.
11.3. Paaiškinkite Kerberos protokolą.
11.4. Paaiškinkite Diffie-Hellmano raktų nustatymo protokolą.
11.5. Paaiškinkite, kaip vykdoma įsiterpimo (man in the middle) ataka.
11.6. Paaiškinkite Diffie-Hellmano rakto nustatymo protokolą su parašais.
11.7. Paaiškinkite bendrais bruožais, kaip sertifikuojami viešieji kriptosistemų raktai.

12. Paslapties padalijimas
12.1. Paaiškinkite paslapties padalijimo su slenksčiu (t, w) schemos sąvoką.
12.2. Kaip paslaptis dalijama ir atkuriama Shamiro schemoje su slenksčiu (w, w)?
12.3. Padalykite paslaptį $s = 3$ trims dalyviams su slenksčiu $t = 2$ panaudoję modulį $p = 7$.
12.4. Kas yra leidimų struktūra?
12.5. Yra trys paslapties dalijimo schemos dalyviai $1, 2, 3$. Leidimų struktūros branduolį sudaro du poaibiai $\{1, 2\}, \{2, 3\}$. Padalykite paslaptį $s = 2$ pagal šią leidimų struktūrą.
12.6. Paaiškinkite Asmuth-Blumo paslapties padalijimo schemą.

13. Netiesioginiai įrodymai ir kita
13.1. Paaiškinkite interaktyvų Irenos įrodymą, kad ji žino diskrečiojo logaritmo reikšmę.
13.2. Paaiškinkite interaktyvų Irenos įrodymą, kad ji žino kvadratinio lyginio sprendinį (Fiat-Shamiro protokolas).
13.3. Paaiškinkite, kaip sukuriamas skaitmeninis banknotas ECash schemoje.
13.4. Išvardykite reikalavimus elektroniniam balsavimui.
13.5. Paaiškinkite bendrais bruožais III elektroninio balsavimo protokolą.
13.3. Paaiškinkite monetos metimo protokolą, kuriame naudojami diskretieji logaritmai.