KRIPTOGRAFIJA IN TEORIJA KODIRANJA

Pomembnejša osnovna vprašanja

Klasični tajnopisi (simetrična kriptografija).
Generator naključnih števil, enkratni ščit in dokazljiva varnost.
Zamenjalni, Vigenerov, afini, Hillov in tokovni tajnopisi.
Statistična kriptoanaliza.
Simetrični tajnopisi, DES, AES, MAC, linearna in diferenčna kriptoanaliza.

Kriptografija javnih ključev (asimetrična kriptografija).
Koncept kriptosistema z javnimi ključi (Diffie in Hellman) in enosmerne funkcije.
Praštevila, gostota praštevil, verjetnostno in pravo testiranje praštevilskosti.
Legendrovi in Jacobijevi simboli, faktorizacija, RSA kriptosistemi.
Končni obsegi, diskretni logaritem, algoritmi za računanje diskretnega logaritma,
ElGamalovi kriptosistemi, eliptične krivulje.
Metoda nahrbtnika, Merkle-Hellmanov kriptosistem.
Zgoščevalne funkcije, celovitost podatkov, družina SHA.
Digitalni podpisi, identifikacija, overjanje, DSA.
Aritmetika velikih števil: metoda kvadriraj in zmnoži,
razširjen Evklidov algoritem, kitajski izrek o ostankih.

Teorija kodiranja.
Linearne kode. Ciklične, BCH in Reed-Salomonove kode.
Osnovne neenakosti za kode (npr. Singletonova meja). Prepletanje kod.

Viri

[1] D. R. Stinson, *Cryptography – Theory and Practice*, CRC Press, 1995 in 2. izdaja 2002. Chapman and Hall/CRC izdaja 2006.

[2] P. van Oorschot and S. Vanstone, *An introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, 1989.

Dodatna literatura

1. E. Bach and J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, MIT Press, 1996.
2. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
1. Računala nove dobe, 1. del, *Presek* **30**/4 (02/03), 226–231.
2. Računala nove dobe, 2. del, *Presek* **30**/6 (02/03), 291–296.
3. Napake niso večne - Presek, zgoščenke, planeti in kode, *Presek* **30**/6 (02/03), 361–366.
4. Klasične šifre in zdravstvena kartica (1. del), *Presek* **33**/1 (05/06), 22–24.
5. Diffie-Hellmanov dogovor o ključu (2. del), *Presek* **34**/1 (06/07), 25–30.
6. ter (3. in 4. del), *Presek* ...

Ta in podobna literatura je dostopna na `lkrv.fri.uni-lj.si`

Podrobnejša vprašanja pri predmetu KITK 1,2, razdeljena po področjih:

0. Uvod
1. Klasična kriptografija
2. Shannonova teorija
3. Simetrični kriptosistemi
4. RSA sistem in faktorizacija
5. Drugi javni kriptosistemi
6. Digitalni podpisi
7. Zgoščevalne funkcije
8. Upravljanje ključev
9. Identifikacijske sheme
10. Kode za overjanje
11. Deljenje skrivnosti
12. Psevdonaključna zaporedja
13. Dokazi brez razkritja znanja
14. Uvod v računalniško varnost
15. A. Dokaz izreka o gostoti praštevil
16. B. Osnove teorije kodiranja
17. C. Hadamardove matrike

0. **UVOD:** osnovna delitev kriptologije (kriptoanaliza/kriptografija), osnovni problemi (Kerckhoffov princip, zasebnost, celovitost, overjanje, identifikacija, preprečevanje zanikanja, protokoli,...) in osnovna področja, širši kontekst, gradniki, pametne kartice (in drugi varnostni žetoni), biometrika;

1. **KLASIČNA KRIPTOGRAFIJA:** zgodovina (jeziki, pisave,...), prikrite šifre, zamenjalna šifra (pomična, afina), transpozicijske šifre, definicija simetrične šifre, Vigenerejeva šifra (indeks naključja), kongruence, osnovni napadi (4), definicija tokovne šifre (periodičnost, LFSR, RC4);

2. **SHANNONOVA TEORIJA:** varnost (računska, brezpogojna, dokazljiva), enkratni ščit, entripija (lastnosti, pogojna);

3. **SIMETRIČNI KRIPTOSISTEMI:** produktne šifre,
bločne šifre (DES, Rijndael/AES, iteracije, SPN, Feistelova šifra), načini delovanja (ECB, CBC, CFB, OFB), napadi (računska zmogljivost, 2-DES/3-DES/DESX), diferenčna analiza, linarna analiza, implementacijske napadi (DPA, DFA,...),

4. **RSA SISTEM IN FAKTORIZACIJA:** problemi simetrične kriptografije (upravljanje ključev) in koncept asimetrične kriptografije (digitalni podpis, hibridne sheme), teorija števil in končnih obsegov (linearna diofantska enačba, Evklidov algoritem, binarni algoritem, KIO, Lagrangev izrek, Eulerjeva funkcija, Fermatov in Eulerjev izrek), RSA (opis, implementacija - kvadriraj in zmnoži, gostota praštevil) generiranje praštevil (Eulerjev kriterij, Legendrov in Jacobijev simbol, Solovay-Strassen algoritem in MonteCarlo algoritem, Gaussov izrek in Eisensteinova lema, Miller-Rabinov test), napadi na RSA faktorizacija (LasVegas algoritem z odšifrirnim eksponentom, osnovni algoritmi - Pollardova metoda $p-1$, kvadratno rešeto);

5. **DRUGI JAVNI KRIPTOSISTEMI:** DH-algoritem za dogovor o ključu, shema Massey-Omura, problem diskretnega logaritma (DLP - metoda mali-veliki korak, Pollardova rho-metoda, Floydov algoritem, Pohlig-Hellmanov algoritem, metoda index-calculus), končni obsegi (Zechlog tabela, polinomska in normalna baza, TPB, ONB), eliptične krivulje ($\mathbb{Z}_p$ in binarna oblika, pravilo za sestevanje in podvojevanje, grupa na eliptični krivulji, Hassejev izrek), Merkle-Hellmanov sistem z nahrbtnikom, Sistem McEliece (kode za popravljanje napak, Hammingova razdalja, nadzorna in dualna matrika, sindromsko odkodiranje, Goppa kode);

6. **DIGITALNI PODPISI:** koncept navadnega in digitalnega podpisa, podpisovanje in šifriranje, reblocking problem, ElGamalove sheme za podpisovanje (varnost, DSA/DSS, prikrit kanal), napadi (z grobo silo, programski, harwarski, dolžine ključev, DSA/ECDSA), enkratni podpisi (Spernerjeva lema, Bos-Chaumova shema), slepi podpisi, podpis brez možnosti zanikanja (Chaum-van Antwerpen), skupinski podpisi, fail-stop podpisi;

7. **ZGOŠČEVALNE FUNKCIJE:** trčenje, šibko brez trčenj, krepko brez trčenj, enosmerne funkcije, paradoks rojstnih dnevov, zgoščevalna funkcija z diskretnim logaritmom, razširitev zgoščevalne funkcije, zgoščevalne funkcije iz simetričnih kriptosistemov, MD4, MD5, SHA, SHA-1,SHA-2 (256,384,512), RIPEMD, HMAC, časovni žigi;

8. **UPRAVLJANJE KLJUČEV:** upravljanje in usklajevanje ključev, sistemi za distribucijo ključev (P2P, Blomova shema, avtentična drevesa, DH-dogovor o ključu, varnost ElGamal-a in DH-problema), certifikati, PKI (center zaupanja - TA), X.509, proces certifikacije, modeli zaupanja (navskrižna certifikacija, strogo in povratno hierahičen model), preklic certifikata (CRL, problemi), sejni ključi (Kerberos, DH-uskladitev ključev), varnost DH (napad srednjega moža), STS protokol, MTI protokoli, samo-overjeni ključi (Giraultova shema), internetne aplikacije (TCP/IP, IETF: IPsec in VPN - SA, OAKLEY, Racoon I, II, SSL, TLS);

9. **IDENTIFIKACIJSKE SHEME:** protokol izziv-odgovor, Schnorrova identifikacijska shema (dokaz brez razkritja znanja), varnost (polnost, uglašenost), Okomotova identifikacijska shema, Guillou-Quisquaterjeva identifikacijska shema, pretvarjanje identifikacijske sheme v shemo za digitalni podpis;

10. **KODE ZA OVERJANJE:** brezpogojna varnost (proti računski varnosti pri MAC), definicija kode za overjanje, varnost (lažna predstavitev in zamenjava), verjetnost prevare, kombinatorične ocene, pravokotne škatle (OA) in latinski kvadrati (LS), MOLS, karakterizacija optimalnih kod za overjanje s pravokotnimi škatlami, TD designi, ocene entropije;

11. **DELJENJE SKRIVNOSTI:** kombinatorični pristop, stopenjske sheme ((t,t), (t,n), dokaz varnosti), strukture dovoljenj in pooblaščene množice (popolnost, monotonost, minimalnost), konstrukcija z monotonim vezjem, vizulane sheme za deljenje skrivnosti (kontrast, 2-načrti, Hadamardove matrike), formalne definicije, stopenjske sheme iz OA, karakterizacija stopenjskih shem in OA, ...;

12. **PSEVDONAKLJUČNA ZAPOREDJA:** kaj je naključno število (Chaitin in Kolmogorov), algoritmična naključna števila, generatorji psevdo-naključnih bitov (krepko psevdonaključno zaporedje), uporaba (enkratni ščit), primeri (LFSR, (k,ℓ)-RSA-generator, $1/P$ generator, Blub-Blum-Shub generator);

13. **DOKAZI BREZ RAZKRITJA ZNANJA:** vohunova dilema, sistemi za interaktivno dokazovanje (polnost, uglašenost), popolni dokazi brez razkritja znanja, zapis, simulator, zapriseženi biti, shema zaobvezanih bitov (prikrivanje, vezava), računski dokazi brez razkritja znanja, argumenti brez razkritja skrivnosti;

14. **UVOD V RAČUNALNIŠKO VARNOST:** privlačnost računalniških goljufij, varnostna politika (kvaliteta informacij, analiza tveganj), pomembnejše grožnje za varnost (zunanji napadi, hadrwarski napadi, maškarada, škodljivi napadi), pregled varnostnih ukrepov (tehnični ukrepi, gesla,...);

A: DOKAZ IZREKA O GOSTOTI PRAŠTEVIL: Riemannova Zeta funkcija, analitični izreki,...

B: OSNOVE TEORIJE KODIRANJA: osnove (razdalja, Singletonova meja, odkodiranje po principu najbližjega soseda), enostavnejše kode (kode s ponavljanjem, Hammingova koda (7,3), primer RS-kode), glavni mejniki teorije kodiranja (Shannon,...), linearne kode (nadzorna matrika, dulana koda, sindrom), ciklične kode, odkodiranje RS-kod (kot poseben primer BCH kod);

C. HADAMARDOVE MATRIKE: definicija, primeri, i dualnost med stolpci in vrsticami, normalizacija in ekivalentnost, za $n > 2$ velja $4 \mid n$), karakterizacija z grafi, geometrijami in kodami, konstrukcije s tenzorskim produktom, konferenčnimi matrikami.