# Teorija kodiranja in kriptografija (2013/2014)

## Seznam vprašanj za ustni izpit

Vsak(a) kandidat(ka) odgovarja na tri vprašanja, iz vsakega od sklopov po enega. Za pozitivno oceno je pri vsakem vprašanju potrebno pokazati vsaj osnovno znanje. Pri obsežnejših vprašanjih bo postavljenih le nekaj od napisanih podvprašanj.

## Kriptografija, I. del

1. Algebra in teorija števil: razširjeni Evklidov algoritem, Eulerjeva funkcija $\varphi$, algoritem kvadriraj in množi. Grupa $\mathbb{Z}_n^*$, računanje v končnih obsegih.

2. Definicija kriptosistema. Klasični kriptosistemi: Cezarjeva šifra, substitucijska šifra, Vigenérjeva šifra, Hillova šifra, permutacijska šifra. Vrste napadov na kriptosisteme: pasivni (z golim kriptogramom, z znanim besedilom) in aktivni (z izbranim besedilom, z izbranim kriptogramom). Primeri napadov na klasične šifre (frekvenčna analiza pri substitucijski šifri, indeks koincidence pri Vigenerjevi šifri, napad z znanim besedilom pri Hillovi in permutacijski šifri). Kerckhoffov princip. Napad z izčrpnim iskanjem ključev. Varnost klasičnih kriptosistemov (pred katerimi od zgoraj naštetih napadov so/niso varni).

3. Splošne bločne šifre z dolžino bloka $n$. Produkt kriptosistemov, prevedljivost in ekvivalenca kriptosistemov. Želene lastnosti bločnih šifer. Substitucojsko-permutacijska omrežja SPN, Feistlove šifre (skica, ideja). Najbolj osnovna zgradba DES in AES (kot Feistlova šifra oziroma SPN z dodano linearno transformacijo), dolžina ključev in dolžina blokov pri DES in osnovni varianti AES. Načini uporabe bločnih šifer: zakaj različni načini uporabe, elektronska kodna knjiga (ECB), veriženje kodnih blokov (CBC), način s števcem (CM).

4. Tokovne šifre: definicija in uporaba. Napadi pri večkratni uporabi ključev pri aditivnih šifrah. Samokodirna šifra. Linearna rekurzivna šifra: dolžina periode, napadi.

5. Varnost kriptosistemov: stopnje varnosti (brezpogojna varnost, absolutna računska varnost, relativna računska varnost), primeri šifer z določeno stopnjo varnost. Lastnost popolne tajnosti: definicija (najprej definicija kriptosistema in verjetnostnih porazdelitev na množicah besedil, ključev in kriptogramov), lastnosti, Shannonov izrek, Vernamova šifra ima lastnost popolne tajnosti.

## Kriptografija, 2. del

6. Kriptosistemi z javnim ključem: ideja in formalna definicija. Kriptosistem RSA: razlaga, dokaz pravilnosti. Uporaba RSA: generiranje parametrov, izrek o gostoti praštevil, Fermatov test, Miller-Rabinov test za testiranje praštevilskosti. Problem faktorizacije naravnih števil, varnost RSA.

7. Zgoščevalne funkcije: definicija, uporaba, želene lastnosti. Odpornost praslik, odpornost drugih praslik, odpornost na trke in zveze med temi lastnostmi. Zahtevnost iskanja drugih praslik, zahtevnost iskanja trkov, paradoks rojstnega dne. Merkle-Damgårdova konstrukcija. Digitalni podpis: ideja, podpis z RSA.

8. Problem diskretnega logaritma: definicija, zahtevnost, algoritem *Veliki korak, mali korak* za iskanje diskretnega logaritma. Iskanje generatorjev ciklične grupe. El-Gamalov kriptosistem, osnovni napadi. Diffie-Hellmanova izmenjava (uskladitev) ključev, napad srednjega moža. Izmenjava ključev s pomočjo certifikatov (poenostavljeni protokol station-to-station).

9. Infrastruktura javnih ključev: kaj je certifikat (digitalno potrdilo), kako je sestavljen. Vloga certifikatne agencije. Celoten postopek uporabe certifikatov: pridobitev cerifikata, preverjanje certifikata. Primerjava simetričnih in asimetričnih kriptosistemov glede uporavljanja ključev (število ključev za $n$ uporabnikov, problem izmenjave ključev), hibridni kriptosistemi (za izmenjavo ključa uporabimo asimetričen kriptosisem, šifriramo s simetričnim).

## Kodi za popravljanje napak

10. Definicija $(n, M, d)$-koda, Hammingova razdalja, teža. Kaj pomeni, da kod odkrije/popravi $s$ napak? Koliko največ napak lahko odkrije/popravi $(n, M, d)$-kod (utemeljite)? Ekvivalentni kodi.

11. Prenos sporočil po kanalu s šumom (sporočilo $\rightarrow$ kodna beseda $\rightarrow$ prejeta beseda $\rightarrow$ kodna beseda $\rightarrow$ sporočilo). Dvojiški simetrični kanal. Različna pravila za dekodiranje (pravilo največje verjetnosti, pravilo najmanjše napake, pravilo najbližjega soseda) in povezave med njimi.

12. Linearni kodi: definicija, generatorska matrika, nadzorna matrika. Razmaknjenost pri linearnih kodih: ugotavljanje s pomočjo teže kodnih besed, ugotavljanje s pomočjo nadzorne matrike. Dekodiranje s sindromi. Časovna zahtevnost obeh načinov dekodiranja glede na dolžino kodnih besed in glede na razmaknjenost koda.

13. Meje za kode: Hammingova, Gilbert-Varshamova, Singeltonova meja. Ideje dokazov. Popolni kodi: definicija, Hammingovi kodi.

14. Ciklični kodi: definicija, predstavitev s polinomi. Konstrukcija cikličnih kodov s pomočjo generatorskega polinoma. Generatorska matrika pri cikličnih kodih.

15. Reed-Solomonovi kodi: definicija, razmaknjenost - ideja dokaza.

16. Entropija diskretne slučajne spremenljivke, informacijska zmogljivost koda, kapaciteta komunikacijskega kanala, kolikšna je največja informacijska zmogljivost, da lahko sestavimo kod ki bo prenesel kodno besedo s poljubno natančnostjo? (Shannonov izrek: informacijska zmogljivost mora biti manjša od kapacitete komunikacijskega kanala).