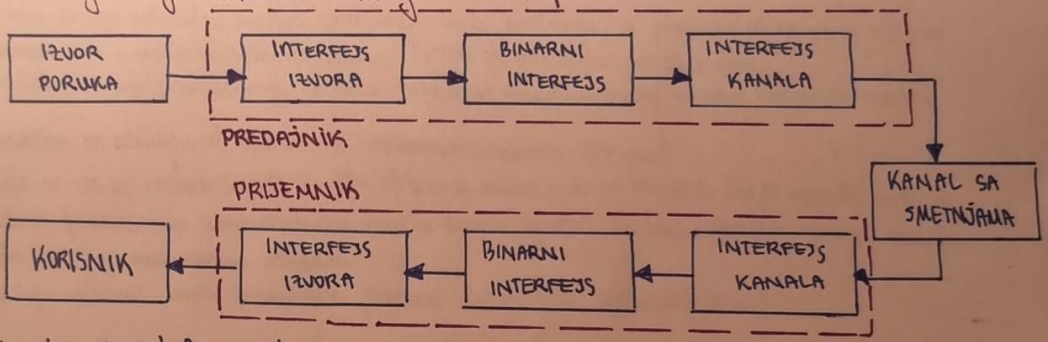
(PNT) PREPORUČENA PITANJA

1. Osnovni elementi: predajnik, kanal, prijemnik

- Predajnik (transmitter) generiše signale poruke, opisuje te signale (sa određenom preciznošću) skupom simbola tj. konvertuje signal poruke iz izvora u formu pogodnu za prenos kanalom
- Kanal (channel) je medijum za prenos (žica, atmosfera, ...).
  Tokom prenosa signal slabi i izobliči se (šum i smetnje iz drugih izvora se superponiraju na signal na izlazu iz kanala) pa prijemniku stiže izobličena verzija.
- Prijemnik (receiver) vraća signal u originalni oblik reprodukcijom originalnih simbola.
  Rekonstruiše originalni signal poruke sa određenom degradacijom kvaliteta.

2. Blok šema digitalnog telekomunikacionog sistema + opis blokova



Izvor i kanal imaju interfejs razdvojen binarnim interfejsom koji vrši obradu i skladištenje podataka. Binarni interfejs omogućava i spajanje podataka iz različitih izvora jer se svi posmatraju kao sekvenca binarnih simbola.

* Izvor poruka: ↪ diskretan (štampan tekst, 0 i 1 niz)
↪ kontinualni (govor, muzika, video snimak)

3. Klasifikacija telekomunikacionih signala – vremenski oblik i spektralne karakteristike.

- Vremenski oblik: 1. Kontinualni: vrednost signala definisana u svakom trenutku (govor, audio, video)
  2. Diskretni: vrednost specificirana samo u pojedinim trenucima
  (npr slova iz alfabeta, binarni simboli od kojih je sastavljena datoteka)
- Spektralne karakteristike: 1. Analogni: amplituda uzima bilo koju vrednost u određenom opsegu
  2. Digitalni: amplituda uzima konačan broj vrednosti iz skupa (_ _ _ _)

4. Šta je digitalizovanje signala, kako se obavlja i zašto je bitno?

- U interfejsu izvora se radi pretvaranje poruka u digitalan signal → digitalizovanje signala (u 0 i 1)
- Prvo se obavlja diskretizacija analognog signala (rez: niz realnih br. koji odgovaraju amplitudama).
- Niz realnih brojeva se zaokružuje na vrednosti iz konačnog skupa (na konačan broj nivoa označen sa
  i time se signal digitalizuje → višenivoski digitalni signal.
- Svaki od q nivoa predstavimo kombinacijom bita 0 i 1 pa se svaki digitalni signal može dalje pretvoriti u binarni digitalni signal.

- Bitno jer je digitalizovan signal "čitljiv" računaru i tako može da se prenese.

6. Opšte karakteristike kanala. Usled čega je signal na izlazu izobličen?

- Kanal je medijum za prenos, unosi slabljenje pri prenosu signala.
- Izobličenje signala se javlja usled ograničenog propusnog opsega ili kao posledica nelinearnosti
  Javljaju se i simetrije kao posledica rada uređaja i opreme, npr šum (internih i eksternih izvora)

7. Koja je mera kvaliteta pri prenosu analognog, a koja pri prenosu digitalnog signala

Analogni: Odnos signal/šum: signal-to-noise ratio (S/N ili SNR)
Digitalni: Verovatnoća greške po bitu (bit error rate, BER)

7. Osnovni telekomunikacioni resursi. Objasniti pojam širine propusnog opsega.
Od čega zavisi maksimalna brzina pouzdanog prenosa informacija?

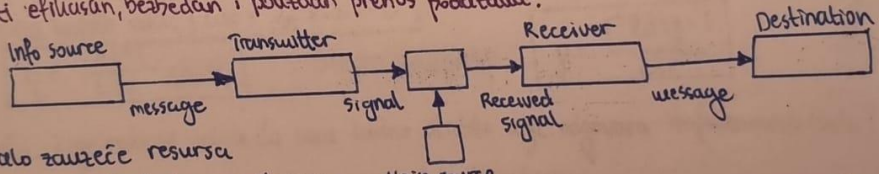
1. Emitovana snaga signala (transmitted power) je srednja snaga signala na predaji (ulazu u kanal)
2. Propusni opseg kanala (channel bandwidth) je opseg frekvencija dodeljen za prenos poruke.

- Emitovanu snagu ne valja mnogo povećavati zbog zračenja, a propusni opseg je ograničen na nacionalnom i međunarodnom nivou. Širina je analogna prečniku cevi.
- Maksimalna brzina pouzdanog prenosa kroz dati medijum zavisi od oba osnovna resursa.

8. Kakve osobine se očekuju od savremenih telekomunikacionih sistema?

- Očekuje se da se resursi koriste na što efikasniji način i da se obezbedi što je moguće brži ali pouzdan prenos (sa kontrolisanim, malim nivoom greške) za malo zauzeće resursa kanala sa što manjom emitovanom snagom.
- Današnji sistemi umeju pouzdano prenose čak i kroz nepouzdan kanal

9. Blok šema sa stanovišta teorije informacija. Na šta se misli kada se kaže da je cilj obezbediti efikasan, bezbedan i pouzdan prenos podataka?



Efikasan: Malo zauzeće resursa
Bezbedan: bez mogućnosti kompromitovanja
Pouzdan: dodavanjem redundanse na pametan način se obezbeđuje smanjenje ranjivosti

10. Pojam informacije i njena kvantitativna predstava.
Razlike između izvora bez memorije i izvora sa memorijom.

- Značenja informacije: • sintaktički nivo: poruka nosi info ako nije unapred poznato koja će poruka biti emitovana, tj. ako na strani prijema postoji neizvesnost
  • semantički nivo: zahteva se da korisnik razume i značenje poruke (da shvati)
  • pragmatički nivo: razmatra se vrednost informacija tj. korist koju izvlači korisnik

- Količina informacija: $Q(s_i) = \log\left(\frac{1}{P(s_i)}\right)$ Skup simbola $S = \{s_1, s_2, \dots, s_q\}$
  verovatnoće pojavljivanja: $P(s_i)$, $i = 1, 2, \dots, q$

- Izvor bez memorije: opisan skupom S i verovatnoćama $P(s_i)$. Ne postoji jasna pravilnost između uzastopno emitovanih simbola (kod izvora sa memorijom ovde postoji nekakva pravilnost i zavisnost)

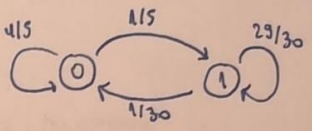
11. Entropija izvora bez memorije.

Entropija je srednja količina informacija koju emituje izvor po poruci, tj. mera neizvesnosti o poruci koju će izvor emitovati.

$$H(S) = \overline{Q(s_i)} = \sum_{i=1}^{q} P(s_i)Q(s_i) = \sum_{i=1}^{q} P(s_i)\cdot ld\left(\frac{1}{P(s_i)}\right) = -\sum_{i=1}^{q} P(s_i)\cdot ld P(s_i) \quad \left[\frac{sh}{simb}\right]$$

12. Entropija izvora sa memorijom prvog reda, dijagram stanja. Primer izvora sa memorijom.

$$H_1(S) = \sum_{j=1}^{q}\sum_{i=1}^{q} P(s_i,s_j)\, ld\left(\frac{1}{P\left(\frac{s_i}{s_j}\right)}\right)$$



Primer: Govor tj. štampan tekst ili senzor parking mesta koji očitava da li je mesto zauzeto svakog minuta.

13. Pojam statističkog koda. Hafmenov kod. Pojam kompaktnog koda.

- Statistički kodovi predstavljaju preslikavanje pojedinačnih simbola (ili njihovih kombinacija) u sekvencu simbola kodne liste, to je skup kodnih reči. To je kod koji možemo kompresovati ako znamo verovatnoće pojavljivanja simbola ili određenu pravilnost pojavljivanja simbola.
- Hafmenov kod je praktičan kod za kompresije optimalan za izvor bez memorije, sa konačnim brojem simbola čije su verovatnoće poznate. On garantuje dobijanje kompaktnog koda.
- Kompaktan kod je kod čija je srednja dužina kodne reči ≤ srednje dužine svih ostalih trenutnih kodova za isti izvor i istu kodnu listu. Ne postoji druga komb. kodnih reči tako da kod bude trenutan a ef. veća.

14. Srednja dužina kodne reči, efikasnost, stepen kompresije. ! L_{sr} ne može biti manja od entropije !

Srednja dužina kodne reči: $L_{sr} = \sum_{i=1}^{q} P(s_i)\cdot l_i$

Efikasnost: $\eta = \frac{H(S)}{L_{sr}}\cdot 100\%$ Stepen kompresije: $\rho = \frac{\lceil ld(q)\rceil}{L_{sr}}$

15. Kodno stablo. Koje osobine mora da ima kodno stablo koje odgovara Hafmenovom kodu?

- Ako se simboli pridružuju isključivo listovima, kod je trenutan.

Hafmenovo kodno stablo (kodovanje sa 2 simbola) ima sledeće osobine:

1. Simboli sa ↑ verovatnoćom se nalaze bliže korenu, to su uvek susedni čvorovi
2. Čitajući čvorove s leva udesno i od najvišeg nivoa ka korenu nam daje čvorove sortirane u neopadajućem poretku → sibling property (osobina izdanka)

16. Kako se vrše proširenja izvora i koji je njihov značaj? Kolika je maksimalan stepen kompresije izvora bez memorije?

- Ako se umesto pojedinih simbola posmatraju sekvence od 2, 3 ili više sukcesivnih simbola tada posmatramo n-to proširenje izvora. Obeležava se S^n, broj simbola je q^n.

Može da bude efikasnije nego prvo dužnog Hafmena (npr za samo dva simbola → $H^2(S)$: $\eta = 97{,}38\%$ a Huff $\eta = 88\%$

- Maksimalni stepen kompresije se postiže kada je srednja dužina kodne reči jednaka entropiji izvora, tj. iznosi $\rho = \frac{\lceil ld(q)\rceil}{H(S)}$

17. Formulacija i komentar prve Šenonove teoreme.

Teorema: Dovoljnim proširivanjem reda izvora i njegovim kodiranjem može se postići proizvoljno visoka efikasnost (Lsr da se približi entropiji izvora)

$$\lim_{n\to\infty} \frac{L_{sr,n}}{n \cdot H(S)} = 1$$

Ova teorema daje odgovor na pitanje koji je minimalni broj simbola kojim se može predstaviti poruka a da se pritom ne izgubi informacija.

Npr: za dovoljno veliko proširenje 100 simbola izvorne liste menjamo se malo više od 8 simbola kodne liste bez gubitka informacija.

18. Kodovi zasnovani na korišćenju rečnika. Lempel-Zivov kod.

Kodovi koriste rečnik koji sadrži kodne reči za određene sekvence simbola i na osnovu rečnika kodiju odnosno dekodiraju poruku.

Ovako radi i LZ algoritam koji se sastoji iz dve faze:

1. Formiranje rečnika na osnovu dela sekvence koju emituje izvor
2. Koristi formiran rečnik za kompresiju ostalog dela sekvence koje emituje izvor.

19. Zaštitni kodovi (kodovi za kontrolu grešaka). Blok kodovi, kodni količnik.

- Zaštitni kodovi smeštaju poslate poruke u "pakovanje" koje ih štiti od štetnog uticaja kanala.
- Blok kodovi su metod unošenja redundanse koji je najlakše razumeti i realizovati

Generiše ih blok koder - prihvata k bita i predstavlja ih odgovarajućom kodnom reči dužine n bita. Zbog grešaka se unosi redundansa pa mora da važi $n>k$.

- k info bita $(i_1, i_2, \dots, i_k)$ i n-k kontrolnih bita $(z_1, z_2, \dots, z_{n-k})$

- Veličina $R = \frac{k}{n}$ je kodni količnik blok koda (n,k), to je udeo informacionih bita u kodnoj reči.

20. Kod sa ponavljanjem, dve moguće realizacije dekodera i verovatnoća greške koju vidi korisnik.

- Svaka 0 na ulazu kodera se pretvara u niz od n 0 na izlazu kodera, isto tako 1 u niz od n 1ica

- Realizacije dekodera: 1. 000 i 111 se dekodiraju kao 0 i 1 respektivno

$M=2$
$n=3$

U svim ostalim slučajevima se smatra da su nastale greške

Verovatnoća greške $P_e = p^3 = 10^{-6}$ (p^n)

2. Pravilo većinskog odlučivanja: više nula → 0, više 1ica → 1

Verovatnoća greške: $P_e^{(2)} = \binom{3}{3}p^3 + \binom{3}{2}p^2(1-p)$ $\sum_{t=\lfloor n+1/2 \rfloor}^{n} \binom{n}{t} p^t (1-p)^{n-t}$

21. Ispravljanje i detekcija grešaka, FEC i ARQ pristup.

- FEC (Forward error correction): detektuje grešku i ispravlja taj jedan bit (većinsko odlučivanje)
- ARQ (Automatic Repeat request): detektuje ali ne ispravlja grešku već putem povratne sprege kaže koderu da pošalje reč sa greškom ponovo.

22. Formulacija druge Šenonove teoreme. Prokomentarisati njen značaj.

- Dok god je kodni količnik manji od parametra Imax može se naći takav zaštitni kod da se verovatnoća greške proizvoljno smanji. Moguć je pouzdan prenos kroz nepouzdan kanal.
- Teorema daje odgovor na pitanje koja je max V prenosa kroz kanal u kome postoje smetnje

$$I_{max} = 1 - (1-p)\cdot ld\left(\frac{1}{1-p}\right) - p \cdot ld\frac{1}{p}$$

23. Objasniti konstrukciju Hemingovog (7,4) i Hemingovog (8,4) koda

Šablon: 1 00(1) z1 — Tražimo poziciju prve jedinice u kolonu od najnižeg bita i tu postavljamo zaštitne bitove.
2 0(1)0 z2
3 011 i1 — Preostale jedinice kolona određuju kontrolne sume:
4 (1)00 z3
5 101 i2 $z_1 = i_1 \oplus i_2 \oplus i_4 = 1$
6 110 i3 $z_2 = i_1 \oplus i_3 \oplus i_4 = 0$
7 111 i4 $z_3 = i_2 \oplus i_3 \oplus i_4 = 0$

$I = [1101] \longrightarrow X = [\underset{(3)}{1}0\underset{(5)}{1}\underset{(6)}{1}0\underset{(7)}{1}]$ Npr. greška na 6. poziciji $\Rightarrow Y = [1010(1)1]$ ide u dekoder

Dekodovanje se obavlja pomoću sindroma: $s_1 = y_1 \oplus y_3 \oplus y_5 \oplus y_7 = 0$
$s_2 = y_2 \oplus y_3 \oplus y_6 \oplus y_7 = 1$
$s_3 = y_4 \oplus y_5 \oplus y_6 \oplus y_7 = 1$
y koji se sabiraju su mesta nečeva u datim kolonama.
↑ S[110] = 6 Pozicija greške otkrivena invertujemo šesti bit.

- Ako je grešaka na više bitova, dekodovanje može da pogorša performanse
Dakle, kod (7,4) detektuje i koriguje samo kada postoji jedna greška.
- Kod (8,4) ima dodat bit parnosti na kraju koji je jednak sumi ostalih 7b kodirane reči

$z_4 = \sum_{i=1}^{7} x_i \qquad s_4 = \sum_{i=1}^{8} y_i \Rightarrow$

S=0, s_4=0: nema greška
S>0, s_4=1: neparan broj grešaka, sindrom pokazuje poziciju
S>0, s_4=0: paran broj grešaka
S=0, s_4=1: greška baš na bitu parnosti

24. Skraćeni Hemingovi kodovi - objasniti konstrukciju koda (6,3).
- Izostavljaju se pojedini informacioni biti

1 00(0)1 K_1
2 00(1)0 K_2
3 0011 1
4 0(1)00 K_3
5 0101 z_2
6 0110 i_3

25. Hemingovo rastojanje, Hemingova težina i sposobnost koda da ispravlja / detektuje greške
- Hemingovo rastojanje d je broj bita u kojima se razlikuju dve kodne reči iste dužine (broj 1 u sekvenci grešaka)
- Hemingova težina je broj jedinica u zbiru dva koda
- Min. H. rastojanje se određuje tako što se odrede svi parovi reči i odrede se njihova rastojanja
To je min. broj 1 u sekvenci grešaka koji će dovesti do toga da greška ne bude otkrivena.

Korigovanje: $d_{min} \leq 2e_c + 1$ Detekcija: $d_{min} \leq e_c + e_d + 1$ $e_c \rightarrow$ corrected
$d \geq 2e_c + 1$ $d \geq e_c + e_d + 1$ $e_d \rightarrow$ detected

26. Linearni blok kod. Način opisa pomoću generišuće matrice.
- LBK je vektorski potprostor VP-a nad poljem GF(q), q → broj simbola. Ukupno sve 2^k elemenata (..., k)
- Baza je skup k nezavisnih kodnih vektora koji generišu ceo kodni potprostor i mogu se složiti u oblik generišuće matrice dimenzija k.n.
- Proces kodovanja je jednostavan: $C = i \otimes G$ ⊗ → matrično množenje pomoć 2

4. Predstava Hemingovog koda pomoću generišuće matrice, kontrolne matrice i grafa

Heming [7,4]

$$G = \begin{bmatrix} 1 & 1 & \textcircled{1} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & \textcircled{1} & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & \textcircled{1} & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & \textcircled{1} \end{bmatrix}$$

Info bitovi → 3, 5, 6, 7

Kolone 1, 2 i 4 određuju zaštitni bitovi

$z_1 = i_3 \oplus i_5 \oplus i_7$ => kčevi 11, 12 i 14 pozicije

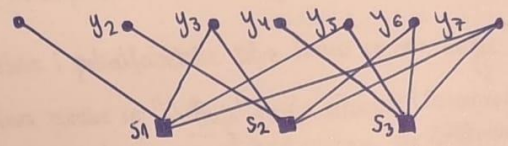
Kodna reč se dobija kada se informaciona reč pomnoži generišućom matricom.

Kontrolne sume → kontrolna matrica

$$s_1 = y_1 + y_3 + y_5 + y_7$$
$$s_2 = y_2 + y_3 + y_6 + y_7$$
$$s_3 = y_4 + y_5 + y_6 + y_7$$

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Tanerov graf:



28. Interliving, način rada matričnog interlivera i deinterlivera.

- Koristi se kada se greške u kanalu pojavljuju u paketima koji se popravljuju retko. Formirane kodne reči se ne šalju sukcesivno na kanal već se čuvaju u memoriji u interlivere Kad se upiše određen broj reči (ℓ^2) onda se šalju najpre prvi biti reči, pa drugi, itd.. Po kolonama. Time se paketska greška prostire u više koraka i moguće je otkloniti je.
- Deinterliver prima reči i upisuje ih po kolonama i ispravlja ih, pa ih čita i šalje po vrstama
- Ako je paket grešaka $< \ell$ moći će da se ispravi greška u svim rečima, ako je $> \ell$ onda neće

29. Šta je ciklični kod (objasniti pojam)? Šta je iterativno dekodovanje?

- Ciklični kod je kod čijom se cikličnom permutacijom udesno dobijaju sve kodne reči određenog LBK. Opisuje se generišućim polinomom čiji su koeficijenti određeni jednom vrstom generišuće matrice

$$G = \begin{bmatrix} \textcircled{1} & 0 & \textcircled{1} & \textcircled{1} & 1 & 0 & 0 \\ 0 & \textcircled{1} & 0 & \textcircled{1} & \textcircled{1} & 1 & 0 \\ 0 & 0 & \textcircled{1} & 0 & 1 & 1 & 1 \end{bmatrix}$$

g

$g = (1011) \Rightarrow g(x) = 1 + x^2 + x^3 + x^4$

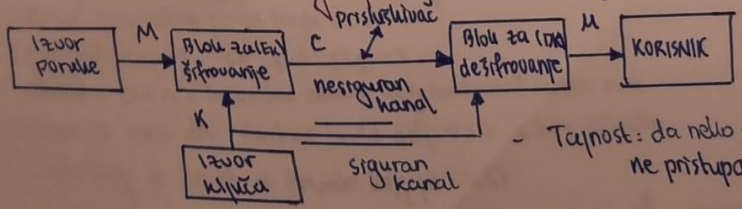
$c(x) = i(x) \cdot g(x)$ pa prevodimo u kodnu reč C.

- Iterativno dekodovanje je nalik rešavanju ukrštenice, dva čoveka naizmenično rešavaju šta znaju jedan samo vodoravno a drugi samo vertikalno dok se ne reši.

30. Šta je kriptografija a šta kriptoanalizа?

Kriptografija je nauka o konstrukciji šifara a kriptoanaliza nauka o "razbijanju" šifara

31. Osnovna blok-šema simetričnog kriptosistema. Šta je tajnost a šta autentičnost?



- Tajnost: da niko neovlašćen/nepozvan ne pristupa podacima

- Autentičnost: sigurnost da su primljeni podaci primljeni od osobe od koje očekujemo da ih je poslala mama

32. Objasniti šifru transpozicije. Kako se ona može razbiti?

Blok simbola se unosi po određenom pravilu u neku (obično) 2D geometrijsku figuru, npr. matrica i zatim se iščitava po određenom pravilu.

TELEKOMUNIKACIJE: TELE KOMU NIKA CIJE
permutacija 3142: LTEE MKUO KNAI JCEI

ili:
TELE
KOMU
NIKA
CIJE

Vrste matrice se čitaju po permutaciji 3142

LMKJ TKNC EUAE EOII

Razbijanje se postiže anagramiranjem (svojstveno posmatranom jeziku)
Traži se takvo premeštanje slova da se pojave reči ili delovi reči.

33. Objasniti monoalfabetske i polialfabetske šifre. Kako se one mogu razbiti?

- Monoalfabetska: Sva slova poruke se "shiftuju" zadatu vrednost (Cezarova šifra) i ključ je jedno slovo
  Npr 3=G i to oduzimamo od kriptograma pri dešifrovanju.

  Razbijanje: statistikom pojavljivanja pojedinih slova, treba 25 slova u eng. jeziku

- Polialfabetska (Vižnerova) šifra: Periodične različite proste zamene
  Npr TELEKOMUNIKACIJE pomoću reči KLJUČ se K=4 periodično šifruje.

  Razbijanje: Mora se utvrditi period ponavljanja (dužina ključa).
  Traže se identični trigrami ili duži blokovi i pretpostavlja se da je
  dužina ključa najmanji zaj. činilac pronađenih rastojanja trigrama.

34. Šta je to Vernamova šifra? Zašto je ona bitna i koji su njeni nedostaci?

- Šifra kod koje se kao ključ koristi potpuno slučajan niz slova čija je dužina jednaka dužini poruke.
- Ako se za svaku poruku bira druga sekvenca kao ključ onda se stvarno dobija izuzetna šifra koja se teorijski ne može razbiti, ali zahteva određene memorijske resurse pa se ne može često promenjivati

35. Ukratko objasniti Diffi-Helmanov algoritam.

- Predstavlja primer asimetričnog kriptosistema.
- Osobe A i B žele da se dogovore o jednom tajnom slučajnom elementu u cikličnoj grupi G, kojeg bi posle mogli koristiti kao ključ za šifrovanje u nekom simetričnom kriptosistemu.
  g → generator
  Obe osobe generišu slučajan prirodan broj iz $\{1,2,\dots,|G|-1\}$ i šalju jedna drugoj element g^a ili g^b.
  Osoba A izračuna $(g^b)^a = g^{ab}$, Osoba B izračuna $(g^a)^b = g^{ab}$ i tajni ključ je $K = g^{ab}$
  Sve operacije idu modp ($g < p-1$)

36. Ukratko objasniti RSA algoritam. Kako se mogu kombinovati simetrični i asimetrični kriptosistem?

1. Izabrati dva velika prosta broja P i Q
2. Izračunati $n = p \times q$, $z = (p-1) \times (q-1)$
3. Izabrati e ($e < n$) tako da nema zajedničkih faktora sa z
4. Izabrati d tako da $e \times d - 1$ bude deljivo sa z bez ostatka
5. Public key je (n,e) a Private key je (n,d)

Da se šifruje poruka m: $c = m^e \bmod n$ $\quad m=12,\ m^e = m^5 = 1524832,\ c = m^5 \bmod 35 = 17$

Dešifrovanje sekvence c: $m = c^d \bmod n$ $\quad c = 17\ \ c^d = c^{29} = \dots,\ m = c^{29} \bmod 35 = 12$