**10. Komunikacija između procesa**

**Ovaj dokument se izvorno nalazi na** <https://docs.google.com/document/d/154tfehzFj5iIqmPYHYOUDDjY0WtimejFXEuHahnNiik/edit>

**U OVOM DOKUMENTU SU SKUPLJENA SVA PITANJA SA PRIJASNJIH MI-eva**

**Studenti koji su slusali NOS 2016/2017 su kreirali ovaj dokument i ova kopija sluzi samo kao backup u slučaju da se dokument sa linka izgubi.**

1. **Poruka se ne šalje izravno procesu nego:**

U red poruka

1. **Što se dodaju na IP razini?**

adresa odredišta i izvorišta

1. **Ako redom poruka glumimo semafor onda funkciji čekaj\_semafor odgovora:**

uzimanje\_iz\_reda( btw. postavi\_semafor -> stavljanje\_u\_red)

1. **Prema pravilima gl. logičkog sata proces povećava svoj log. sata kada?**

/\* između svaka dva događaja \*/

1. Izmedu svaka svoja 2 karakteristicna dogadaja
2. Po primitku poruke
3. **Kako se osvježava vrijednost lokalnog log. sata? (Cj=max...)**

Cj = max {Cj(prijašnji), Tm}+1 gdje je Tm Ci od procesa koji je poslao zahtjev

1. **Koliko se poruka razmjeni u Ricart-Agrawalinom protokolu ako je N čvorova?**

2\*(N-1) (ako bude pitanje koliko točno kojih, N-1 ZAHTJEVA I N-1 ODGOVORA)

1. **Koliko poruka u Lamportovom protokolu, 10 čvorova.**

3\*(N-1) = 27

1. **Čitanje cjevovoda je za razliku od čitanja datoteke:**

destruktivno

1. **Okolina (u kontekstu var. okoline) je:**

niz znakova "ime=vrijednost" koji se predaje svakom programu prilikom pokretanja

1. **Neimenovan cjevovod ima koliko opisnika:**

dva

1. **Ako je vrijeme 712, a primi poruku 718, onda je nova vrijednost sata: (brojeve napamet bacam)**

C = max {712,718}+1=719

**12. a) Lamport, kada želi ući onda svima šalje i stavlja u svoj red:**

stavlja u svoj red zahtjev(i,T(i))

**b) Kada primi tu poruku onda napravi:**

-namjesti svoj sat prema pravilima GLS-a

-u svoj red čekanja stavlja zahtjev i šalje odgovori(i,T(j)) procesu Pi gdje je T(j) = novi Cj

**13. Ricart-Agrawalin, zadano C1,C2,C3, P1 želi ući, koji se poruke razmjenjuju i stanja logičkih satova po ulasku u KO**

Sličan je primjer 10.3 u knjizi i u predavanjima na materijalima.

**14. U postupku povezivanja cjevovoda na standardni ulaz treba zatvoriti standardni ulaz ili izlaz?**

ulaz

**15. Prema pravilima globalnog logičkog sata kada proces šalje poruku on uz nju pridodaje**

svoj ID procesa i vrijednost lokalnog logičkog sata

**16. Na koju će vrijednost postaviti lokalni logički sat proces ako primi poruku s vremenskom oznakom 178, a vrijednost njegovog logičkog lokalnog sata je 177?**

max(178, 177) + 1 = 179

**17. Navesti broj poruka koji treba razmijeniti u sustavu s 10 računala gdje se na svakom računalu nalazi po jedan proces koji se natječe za ulazak u kritični odsječak ako se koristi raspodijeljeni Lamportov protokol:**

● 3 \* (N - 1) -> 3 \* 9 = 27 -> ovo bi bilo ako samo jedan pokusava ući

● 3 \* (N-1) \* 10 -> mora ici puta 10 samo -> 270

**18. Koje informacije u Internet protokolu se dodaju bloku podataka?**

izvorišnu i odredišnu IP adresu

**19. Navedite tri načina na koje dretve različitih procesa mogu komunicirati.**

● razmjenom poruka

● datotekom

● cjevovodi

● uz pomoć dijeljenog spremnika

● uz pomoć varijabli okoline

Ukoliko se radi o raspodjeljenim sustavima, onda samo razmjenom poruka (drugi mehanizmi se osljanjaju na poruke). To su RPC, raspodjeljeni adresni prostor

**20. Okolina (environment) je?**

niz znakova oblika “ime = vrijednost” koji se predaje svakom programu prilikom pokretanjaz

**21. U postupku povezivanja dva procesa uz pomoć reda poruka okolina može poslužiti za razmjenu \_\_\_\_\_ .**

identifikatora reda poruka.

**22. Nedostatci običnog cjevovoda: \_\_\_\_\_**

● procesi moraju biti u srodstvu

● ne može se stvoriti nakon što su stvoreni (child?) procesi (misli se na random stvorene, koji nisu u srodstvu)

● Običan cjevovod ima ograničenu veličinu međuspremnika na 10 stranica (cca 4kB)

**22b. Prednosti imenovanog cjevovoda:**

* Rad s imenovanim cjevovodom odgovara radu s datotekama
* Procesi koji komuniciraju preko imenovanog ne moraju biti u srodstvu
* Nema ograničenja na duljinu (kod običnog je 10 stranica)

**23. S koliko je opisnika opisan IMENOVAN cjevovod?**

jednim

**24. Lamportov protokol, procesi P1, P2 i P3 uz početne vrijednosti C1=12, C2=7, C3=20. P1 i P2 istovremeno pošalju zahtjeve, odredite logičke satove i redove zahtjeva u trenutku kada P1 uđe u kritični odsječak.**

<http://www.deviantpics.com/images/2017/04/24/12.png>

- *da li netko može objasniti zašto u primjeru se mijenja vrijednost satova C2,C3 nakon poruke izlazak?* Zato što dobivaju od procesa P1 poruku Izlazak() a kad dobiju bilo kakvu poruku, ažuriraju svoj lokalni sat

-to ne pise u algoritmu(iako je napomenuto negdje iznad)

**25. Kako se zove mehanizam unutar jednog računala koji broji događaje?**

● lokalni logički sat

**26. Prema pravilima globlanog logičkog sata na koju vrijednost proces Pi postavlja lokalni logički sat kada primi poruku zahtjev(j,T(j))?**

● Ci = max (Ci, T(j)) + 1

**27. Navesti ispravane redosljed koraka ako želimo napraviti cjevovod tako da roditelj čita, a dijete piše u cijevovod:**

1. **U djetetu zatvoriti kraj cjevovoda za čitanje**
2. **U procesu roditelja pozvati stvaranje djeteta**
3. **Stvoriti cjevovod**
4. **U roditelju zatvoriti kraj cjevodova za pisanje**

\_ \_ \_ \_

**28. Isto s cjevovodima ali je bilo sa funkcijama, kojim redosljedom treba nesto napraviti, i koji korak se može preskočiti da bi cjevovod i dalje bio ispravan:**

**Ovakve slične funkcije su bile:**

1. close(1);

2. dup( cj[1] );

3. close( cj[1] );

4. close( cj[0] );

**29. Kako proces može znati da je poruka u redu poruka namjenjena za njega?**

**11. Sigurnost računalnih sustava**

1. **Veličina bloka: DES, 3DES, IDEA, AES**

Veličina bloka / veličina ključa

* DES 64 / 56
* 3DES 64 / 112, 168
* IDEA 64 / 128
* AES 128 / 128,192,256 (129 standard, 128/192/256 je predloženo)

1. **Br. potključeva: DES, OTP, IDEA, AES128**

* DES 16
* OTP - 0 (nemamo potključeve?) -*što je OTP?* -one time pad
* IDEA - 52
* AES128 - 128bit kljuc - 11 ( 192bit kljuc - 13, 256bit kljuc - 15)

šta nije #koraka + 1? Je :D

// kako se iz broja bitova kljuca dobije koliko ima podkljuceva za AES?

**//** podključeva imaš (broj\_koraka + 1) s time da je prvi podključ zapravo originalni ključ

1. **Broj S-kutija kod DES-a:**

DES ima 8 s-kutija

//zna li netko koliko ima S-kutija kod AES-a?

//->1(jedna)

1. **Kod CBC greška uzrokuje grešku u koliko blokova:**

2 - ako je greška u cj bloku, bit će loše dekriptirani blokovi cj i cj+1

1. **Napiši dva načina kodiranja gdje se prethodno kriptirani tekst šalje na ulaz sljedećeg:**

* cfb i cbc

1. **Koja dva načina su kao OTP gdje se…**

OTP = duljina ključa treba bit jednaka duljini poruke koja se kriptira

Načini: CFB, OFB, CTR

1. **phi(17), phi(18), phi(725) ili tako nešto**

phi(17)=16

phi(18=2\*3\*3)=6 *(nije li ovo 4=1\*2\*2)*? Nije, jer formula (q-1)(p-1) vrijedi samo ako broj ima dva faktora. Inace koristis formulu phi(n) = n (1 - 1/p1)(1-1/p2)..., gdje su p1, p2 faktori od n. Da ali, 18 \* (1 - ½)(1-⅓) = 6 (izracunaj, nije 4 nego 6.sta lazes ovaj napaceni narod? Nemas to pravo)? Svaki faktor gledas jednom. Oh, tnx… mislim da u umnozak ulaze razliciti prosti brojevi .. phi(18) = 6

https://en.wikipedia.org/wiki/Euler%27s\_totient\_function

phi(725=5\*5\*29)=560

~~Eulerova funkcija je multiplikativna, što znači da je phi(a \* b) = phi(a) \* phi(b). Stoga je phi(18) = phi(2 \* 3 \* 3) = phi(2) \* phi(3) \* phi(3) = 4. Source:~~ [~~https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf~~](https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf) ~~teorem 2.11.~~

<http://www.javascripter.net/math/calculators/eulertotientfunction.htm>

phi(18) = 6

**8. Broj koraka u kriptosustavu AES ovisi o:**

●veličini kljuca, ako je 128 onda 10 koraka, ako je 192 onda 12, ako 256 onda 14 koraka

* Šta nije o veličini bloka podataka i veličini bloka ključa - koko sam shvatio, AES može imat samo duljinu bloka ~~4 bajta~~ 128 bita, a izvorni algoritam (Rijndael) može 128, 192, 256 bita ~~4, 6 ili 8~~
* Meni je u blicu bilo ovo pitanje i dobio sam bod za odgovor “velicini kljuca”

**9. Koliko iznosi Eulerova phi funkcija za phi(77)?**

●77=11\*7 -> (p-1)\*(q-1) = 60

**10. Napisati Kerckhoffov princip**

● kriptosustav mora biti siguran i onda kada su sve informacije o kriptosustavu, osim tajnog ključa, svima dostupne

**11. Ako se 100 bajtova kriptira s IDEA, koliko će velika biti kriptirana datoteka?**

●100 \* 8 / 64 -> najveće cijelo -> 104

* (može neko ovo pojasniti?) Mislim u knjizi piše da se kriptirani blok dobiva nadovezivanjem 16 bitnih blokova u 64 bitni kriptirani podatak… pa mi nije baš jasno.
* 100 \* 8= 800 bitova; 800/64 bita po bloku = 12.5 bloka; blokovi su fiksni (ne možemo imati pola bloka) -> 13 blokova; 13 blokova \* 64 bita = 832bita (104 bajta)

**12. U DES-u izlazi svih supstitucijskih tablica spajaju se u podatak veličine**

* 32 bita (jer imamo 8 s-tablica a izlaz svake tablice je 4bita)

**13. U zadnjem koraku u AES-u ne koristi se funkcija**

* pomiješaj stupce.

**14. Koje operacije koristi IDEA**

* -XOR

### -Zbrajanje po modulu 2^16

### -Množenje po modulu 2^16 + 1

**15. Navesti četiri osnovna sigurnosna zahtjeva**

**●** tajnost

● neporecivost

● integritet

● autentičnost

Zapamtite si ko RATNIK, s tim da su osnovni zahtjevi ovi srednji: ATNI

Ili kao TINA (katanić)

**16. Četiri funkcije 1337-bitnog AES-a?**

* Zamjena znakova (supstitucijska tablica)
* Posmak redova
* Miješanje stupaca (ovo se izostavlja u posljednjem koraku)
* XOR (za podključ)
* Treba znati operacije zbrajanja i množenja u mijepšanju stupaca za MI (kaže u predavanjima tako)

**17. Koji se načini kriptiranja mogu koristiti za kriptiranje toka podataka?**

* OFB i CFB (i CTR?)

**18. Pet načina kriptiranja?**

* ECB (elektornička bilježnica), CBC, CFB, OFB, CTR (brojač)

19.  (postupak)

Može li netko napisati postupak kako se ovakvi zadatci rješavaju?

<http://pasteboard.co/7VtMIwN6e.jpg>

- treba samo provesti algoritam, moze se rekurzivno i iterativno raditi (u knjizi je iterativni algoritam napisani). Uglavnom imas logN koraka (N je eksponent). Kod rekurzivnog samo cjelobrojno djelis eksponent s 2 dok ne dođeš do nule, a u slucaju da imas ostatak pomnozis sve jos samo sa bazom. (npr. 2^11 = 2^5 \* 2^5 \* 2, pa onda 2^5 = 2^2 \* 2^2 \* 2, 2^2 = 2 \* 2, i onda se samo vratis i imas rjesenje, naravno u svakom koraku sve modulo m racunati). Ovaj rekurzivni postupak nisu spominjali, sigurno je točan pa pretpostavljam da ce priznavati, ali nije bas onak kak su si oni zamislili.

**20. Napisati Kerckhoffov princip**

● kriptosustav mora biti siguran i onda kada su sve informacije o kriptosustavu, osim tajnog ključa, svima dostupne

**21. Digitalni potpis**

● Digitalni potpis: Računa se sažetak poruke te se sažetak poruke kriptira privatnim ključem; sažetak se šalje i kada primatelj primi poruku s javnim ključem pošiljatelja dekriptira sažetak, računa sažetak poruke i uspoređuje ga s onim koji je dobio od pošiljatelja; osiguran je integritet, neporecivost i autentičnost

**22. Ovo je rekao na predavanju da bi moglo biti:**

Modularno eksponenciranje; izračunati metodom uzastopnog potenciranja

353 u **Z**17

Prvo 53 u binarni sustav: 53=110101

53=32+16+4+1

353=332 \* 316 \* 34 \* 31

|  |  |  |
| --- | --- | --- |
| k | l=2k | 3lmod17 |
| 0 | 1 | 3 <- |
| 1 | 2 | 9 |
| 2 | 4 | 13 <- |
| 3 | 8 | 16 |
| 4 | 16 | 1 <- |
| 5 | 32 | 1 <- |

353= 5 u **Z**17 Jer (3 \* 13 \* 1 \* 1) mod 17 = 5

**23. Pronaći prvi broj p veći od 7700 koji prolazi ispitivanje radi li se o prostom broju Fermatovim teoremom. U postupku ispitivanje umjesto proizvoljnog broja nasumično odabranih brojeva a∈Zp\* koristite samo dva broja i to 2 i 7. (ako se za prvi broj 2 utvrdi složenost ne treba provjeravati za drugi broj 7. Napomena. U svim zadacima u ovom ispitu gdje treba izračunati izraz abmod n treba koristiti modularno potenciranje.**

Kako se ovo računa?

Kao ides po svim brojevima poslije 7700 koji nisu ocito slozeni i provjeravas vrijedi li 2^(n-1) = 1 (mod n) i 7^(n-1) = 1 (mod n). Ako oboje vrijedi, broj je prost (ili onaj neki Carmichelov broj)

**24. Digitalna omotnica:**

* Digitalna omotnica: M = (C1, C2), C1 = DES(P, K), C2 = RSA(K, KE), osigurana je tajnost

**12. Miller-Rabin, kako se povećava vjerojatnost pronalaska ispravnog?**

* ispita se Fermatov teorem za više brojeva a
* Osim Fermatovog teorema ispituje se da li za dani broj postoji netrivijalni drugi korijen

x^2 = 1(moda n)

(ako postoji tada je n sigurno složen)

// broj x netrivijalan je drugi korijen od 1 mod n ako je zadovoljena jednadžba x^2≡1 (mod n); ako postoji netrivijalan drugi korijen od 1 mod n, onda je n sigurno složen broj

**13. RSA p=47, q=29, k=3, ključevi?**

● Ke=(5, 1363), Kd=(773,1363)

//kako je ovo izracunato? P\*Q = n = 1363; e\*d = k \* (p - 1)(q - 1) + 1 onda samo trebas pogodit e ili q tako da krenes od najmanjeg prim broja i ispitujes da li zadovoljava jednadžbu. :D

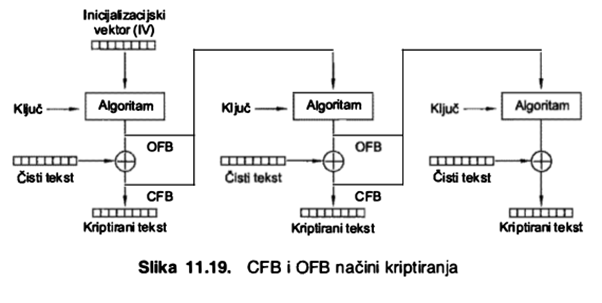
**23. Max veličina bloka u RSA, ako je n=1025**

● 1024? -> Kaj nije log2(n) = 11 bita? // može ovo netko objasnit?

**24. Je li n=1025 ispravno odabran (zanemarimo da je premali broj)?**

● n mora biti umnožak dva prosta broja

**25. Skicirati CFB**



**26. RSA; (n, e) = (55, 7), izračunati sve (n, d). C1=2, kriptirano s javnim ključem, M1=?; C2=3, kriptirano s tajnim ključem, M2=?**

● Odaberu se dva velika prosta broja p i q

● Izračuna se umnožak n = p\*q

● Izračuna se φ(n)= (p-1) (q-1)

● Odabere se e < φ(n) i relativno prost u odnosu na φ(n)

● Izračuna se d < φ(n) tako da bude e \* d = k \* φ(n) +1, e\* d ≡ 1 (mod φ(n))

● Par KE = (e, n) proglašava se javnim ključem

● Par KD = (d, n) proglašava se privatnim ključem

● Kriptiranje: C = E(P, KE) = RSA (P, KE) = Pe mod n

● Dekriptiranje: p = D(C, KD) = RSA - 1 (C, KD) = Cd mod n

● d=23, M1=8, M2=42

RJ:

n=55=11\*5 (p=5, q=11)

phi(n) = phi(55) = (5 - 1) \* (11 - 1) = 4 \* 10 = 40

Vrijedi e \* d = 1 (mod phi(n)) tj

7 \* d = 1 (mod 40) ⇔ 7 \* d = 40 \* k + 1

Tražimo k tdj. Ovo zadovoljeno uz uvjete nzd(phi(n), d) = 1 tj. Da je d relativno prost s phi(n)=40

Napravimo tablicu za k=0, 1, 2,... i faktoriziramo izraz, znamo da jedan faktor mora biti 7 jer je zadano e=7, dobije se za k=4: 161= 7 \* 23 iz čega zaključujemo d=23

Dekriptiranje šifriranog teksta C1 u plaintext M1, koristi se eksponent d za dekripciju, koji je dio tajnog ključa:

M1 = C1^d (mod n) = 2^23 (mod 55) = … modularno potenciranje

**41. DES kriptosustav prije samog kriptiranja generira?**

16 podključeva 6 bajtova (48 bitova)

**50**. **Neka je zadan kriptosustav RSA sa javnim ključem P=(N,e) i privatnim ključem S=(N,d) gdje je N=pq za velike proste brojeve p i q.**

● (1)Za brojeve e i d mora vrijediti:

i. e\*d = k \* phi(n) +1 = 1 mod phi(n)

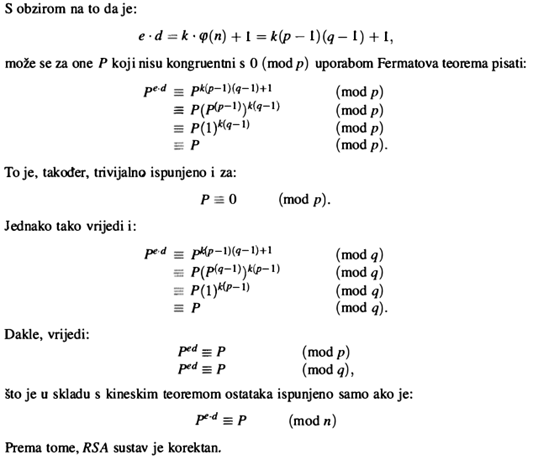
ii. e < phi(n)

iii. d < phi(n)

● 0.5)C=RSA(M,P):

● (0.5) M'=RSA-1(C,S)=

● (1) Dokazati da je M'=M



● Prethodni korak vrijedi samo za brojeve M manje od N koji su relativno prosti sa N. Obrzloži zašto je vrlo teško da se dogodi da slučajno odabrani broj M nije relativno prost za N. \_\_\_\_\_\_\_.

Zato što |zn|\* = (p-1)(q-1), a to je broj brojeva manjih od n koji su relativno prosti s n, a n = pq -> i sansa je (n - |zn|\*) / n = p+q-1 << 1

● Pretpostavimo da se datoteka enkriptira javnim ključem tako da se datoteka podijeli na bajtove B1, B2, ... Bk, svaki bajt se interpretira kao broj između 0 i 255 te se enkriptira pomoću RSA kriptosustava, točnije izračunavaju se brojevi Ci= RSA(Bi, P). Obrazloži efikasan postupak kojim se na temelju javnog ključa i niza C1, C2,..Ck može odrediti sadržaj originalne datoteke.

Modularno potenciranje -> C1 = B1^e mod n je log2(n) slozeno

Sto nije da mozemo mi sami svaki moguci bajt kriptirati javnim kljucem i onda znamo sto znaci svaki Ci koji ovaj salje?

52**. Kolika je maksimalna veličina simetričnog ključa k u bitovima koji može kriptirati RSA kriptosustav u koje je n= 2049? - je li ispravno odabran broj 2049? DA ili NE, objasniti**

● k= 2048, podatak koji kriptiras s RSA mora biti isključivo manji od veličine modula -> k je broj bitova, ovo nije točno onda

-> u teoriji block koji se kriptira mora biti barem jedan bit manji od ključa, dakle za ključe od 2048 bita, max veličina bloka je 2047 bita

**Ana i Branko dijele tajni AES ključ KAB, Ana i Danko dijele tajni AES ključ KAD. Ana želi kriptirati poruku M tako da je mogu dekriptirati Branko, Danko i nitko drugi. Opišite jedan takav mehanizam kriptiranja**

**60. Skicirati CTR način kriptiranja**

**3. AES/DES ulazne i izlazne razlike.**

**2. AES, metoda xPuta().**

**2. (1) Navesti 3 obilježja ključa jednokratne bilježnice.**

Jednak broj bitova poruke i kljuca, svaki put nam je potreban novi kljuc, kljuc se mora generirati slucajno, najsigurniji sustav ali se ne koristi zbog prvo navedenog svojstva.

**3. Niz pitanja od 0,5/1 bod:**

**●(0,5) Kojim sigurnosnim zahtjevom rješavamo lažno predstavljanje?**

**●(0,5) Kojim sigurnosnim zahtjevom rješavamo modificiranje paketa?**

**●(0,5) Kolika je veličina ključa kod 3DES?**

**●(0,5) IDEA-om kriptiramo datoteku od 100 bytea, koliko će biti velika izlazna datoteka?**

**●(0,5) Koliko se S-kutija koristi u DES-u?**

**●(0,5) Koliko rundi se prođe za AES-128?**

**●(1) Dan je decimalan broj kao ulaz u S-kutiju, traži se izlaz (S-kutija je napisana na ispitu).4**

**●(1) Napisati cijelu formulu za 3DES(P,K1,K2,K3).**

Odgovori redom: (izubljen bod, nešto krivo)

● Autentičnost.

● Integritet.

● 112 ili 168.

● IDEA? Pošto se kriptira 64 bita, tj. 8byte, možda je izlaz 104byte? da

● 8.

● 10.

● Pošto nemam S kutiju, nema smisla odgovor, al tamo dobih 0 (prvi stupac, drugi red).

● DES( DES^-1( DES( P, K1 ), K2 ), K3).

**4. (2) Trebalo je pomnožiti 0x17 i 0xA1 uz pomoć funkcije xputa() i polinoma g(x)=x^8+x^4+x^3+x+1.**

B4 → ovo neće bit (jesi siguran? :p) pa nismo to radili, ove godine su to preskočili :P

**5. RSA p=47, g=29, k=3, ključevi?**

rj: (e,n) = (5,1363), (d,n) = (773,1363)

**6. U DES-u izlazi svih supstitucijskih tablica spajaju se u podatak veličine \_\_32?\_\_ bita.**

* 8 tablica sa izlazima po 4 bita = 8\*4 = 32

**MI(24.04.2017) Neka pitanja+ ponovilo se puno toga**

**28. Simetrični kriptoalgoritmi imaju svojstvo da su nužno jednaki (zaokruži točne)**

* **Dužina plaintexta i dužina ključa**
* **Dužina kriptiranog teksta i dužina ključa**
* **Dužina plaintexta i dužina kriptiranog texta (ovo nisam siguran je li ovako bilo)**

**29. Izvorne podatke podjelimo na blokove M veličina 160 bita. Računamo hash na sljedeći način:**

**H = M1 XOR M2 XOR … XOR Mn**

1. **Da li je ovaj algoritam otporan na otkrivanje originala i zašto?**
2. **Ima li kolizija i zašto?**

**30. Zadane dvije datoteke neke duljine. Jedna sadrži random bitove druga samo nule.**

**Ako kriptiramo datoteke sljedećim modovima, da li se samo iz kriptiranih datoteka može skužiti koja je od njih kriptirana? (ii tako nekako)**

1. **ECB**
2. **CBC**

**31. Zadan (N=55, e=27)**

1. **Odredi privatni ključ**
2. **Dektriptiraj poruku (mislim 15)**
3. **Kriptiraj poruku (mislim 17) (uz uzastopno kvadriranje)**
4. **Zašto (N=55 e=6) nije ispravno?**
5. **Zašto (55,11) i (55, 13) nije ispravan par?**

**32.**

**koji je redoslijed(nesto kod stvaranja cjevovoda):**

**a) close(stdout)**

**b) close(CITANJE)**

**c) close(PISANJE)**

**d) dup(nesto)**

**33. Opet neki redoslijed**

**Nesto kao: kakav treba biti redoslijed kada treba stvoriti novi cjevovod u kojem ce dijete slati poruke roditelju**

**a) stvori dijete**

**b) otvori cjevovod**

**c) zatvori za pisanje na roditelju**

**d) zatvori čitanje na djetetu**

**34.**

**U koliko će blokova biti pogreška ako ako se pogreška dogodi u kriptiranom tekstu(tako nesto) i bilo je pitanje za CBC i CFB(ako se ne varam)**

**35. Bio je zadatak sa 3 procesa. u t1 proces P1 i P2 zele uci u kritican odsjecak C1=112, C2=107, C3=120.t2 je trenutku kada proces koji je prvi usao u k.o. Izlazi iz njega. Trebalo je napisati koliko je koji proces poslao i primio poruka u razdoblju izmedu(t1, t2) te koja je vrijednost pojedinog C u trenutku t2. RICART I AGRAWALA**