USMENI ISPIT IZ OTVORENOG RAČUNARSTVA
(pitanja iz prethodnih godina)

Žagar pitanja:

Certificate Authority (CA) :
Certifikat koji govori o potvrdi između osobe i javnog ključa. Taj certifikat se provjerava u CA tijelu.
CA-izdaje certifikate.
Certifikat nam treba da dokažemo primatelju da smo to baš mi.

DTD i XML shema:

DTD – document type definition – definira pravila za oblikovanje XML dokumenata , označava sadržaj i određuje hijerarhijsku strukturu dokumenta – ovo nije XML !

XML shema – extensible markup language shema, defacto ista namjena kao DTD samo što ispravlja brojne nedostatke poput (podrška prostorima imena, definiranje različitih tipova sadržaja elemenata i atributa), - ovo je XML !

Unicode:
Unoicode objedinjuje vise regionalnih normi. On rjesava onaj problem drugih kodnih znakova koji su imali samo ogranicen skup znakova i nisi npr u jednom dokumentu mogla pisati znakove iz razlicitog pisma. Ima mjesta za miljun znakova.

Koje su razlike između DOM-a i SAX-a?
linijsko parsiranje (SAX) – ne stvara reprezentaciju, brz, temeljen na događaju, kad dođe do elementa koji mu treba prekida parsiranje.
potpuno parsiranje (DOM) – objektni model dokumenta, relativno spor, veče opterečenje memorije ali zato readi s potpunim objektom. pogodan za većinu XML-ova.

UTF:
Način zapisa Unicode numeričkih vrijednosti svakog znaka (code point). Postoje tri vrste UTF8, 16 i 32. UTF8 najviše raširen. UTF16-problem poredka, endians, little/big LE / BE, BOM-byte order mark na početku za definiranje poredka.

Posix:
Portable open system interface , potreba za usklađivanjem sučelja operacijskih sustava (programskih, korisničkih i mrežnih)

(X)HTML, CSS, XML, DTD, XSL: svašta o tome (svojstva, razlike međusobne)
-preopširno, naučite :)

Svojstva asinkronog kriptiranja – valjda javni i tajni ključ
Da asinkronog...i sinkronog...stroja :D

Digitalni certifikat – kako se dobiva i koristi:
Certifikat je potvrda u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom. Dakle certifika potvrđuje identitet te osobe. Javan je.
Davatelj usluga certificiranja je pravna ili fizička osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. CA – Certificate Authority izdaje certifikate.

Programski jezici na klijentu koji se izvode u browseru:
Javascript, ActionScript, Python
Na poslužitelju:
PHP , Asp.Net, Java, Python, Perl, Ruby

AJAX i Javascript i razlike među njima:
Javascript - skriptni jezik ugrađen u preglednik; omogućuje dinamičke promjene stranice, i reagiranje na dogadaje; interaktivnost stranice Weba pomoću Javascripta - interaktivan prema korisniku, a za podatke mora dohvaćati čitave stranice.
AJAX - Asynchronous JavaScript and XML, Komunikacija Javascript koda i poslužitelja: asinkroni način komunikacije i sinkroni način komunikacije

Css, cemu sluzi, kako se uklapa u koncept otvorenog racunarstva?
Definiranje rasporeda elemenata na stranici. Definira prikaz podataka. Najčešće se nalazi u vanjskoj .css datoteci te se uključuje u nju u head dijelu, no može biti i unutar same stranice htmla-overriding, ili izravno u sytle atributu elementa.
Često se .css koji je isti za cijelo web sjedište sprema u cache radi brzine.

Pitao Žagar zašto je php dobar, zašto loš, php u odnosu na cgi, što bi da nemam ni php ni cgi.
PHP ima više načina rada: kao dio poslužitelja Weba(modul), kao CGI poveznik kojeg poslužitelj Weba poziva ili iz naredbene linije (CLI - Command Line Interface).
U odnosu na CGI, PHP najčešće se izvodi kao modul poslužitelja Weba

- nema pokretanja dodatnog procesa poveznika
- manje zauzeće resursa (moemorija, procesora)

Kao CGI:

- poslužitelj postavlja varijable okoline isto kao za CGI
- prijenos između poslužitelja i modula nevidljiv je korisniku

PHP je jednostavan, popularan (raširen, puno korisnika), moguća su proširenja, fokusiran na Web
Nedostaci: sporost (interpreter); nedostaci jezika - nepotpun OO model, nekonzistentna podrška za Unicode, podrška prostora imena; nedosljednost API-ja

Da imamo neki dokument kako bi ga tajno prenijeli,tj. on je reko sakrili pa me zbunio:
simetrični asimetrični ključevi. (msm da se asimetrično prenosi ključ, pa se onda simetrično prenosi poruka)

„Počeo sam nešto pričat kako ne možemo biti sigurni da nam stvarno dokument šalje prijatelj, treba nam neki posrednik poput neke ustanove, pa je onda pitao kako možemo neformalnije to izvesti, ispalo da je odgovor da nam je posrednik neki zajednički poznanik, umjesto ustanove, pa kao da nam

treba posrednik za posrednika, pa posrednik za njega i tako ovisi na kolko razina oćeš ići. Pita svakog po malo.“

Kad bi pred sobom imali, recimo, jedan UTF8 znak i UTF16 znak, bismo li vidjeli razliku?
Ako imaš ascii znak, onda je lako. utf8 će imati 1B a UTF16 2B, a ako ne, onda je možda stvar u onom BOMu koji iznačava endianess i dolazi prije poruke, a razlikuje se za utf8 i 16

Koji su ostali primjeri character setova?
ISO 8859, MS Windows ANSI, IBM PC

Što je XML i kako se uklapa u principe otvorenosti?:
XML je jezik za ospi podataka, engl: extensible markup language, problem: ne postoje predefinirana značenja oznaka, strojno i ljudsi OK razumljiv, unosi dosta nepotrebnog koda no i dalje se u velikoj mjeri koristi.

Kad jednom imamo XML podatke, što nam dalje treba?
Treba nam nešto za vizualizaicju, transformaciju i filtriranje tih podataka iz XML-a
Ili možemo s DOM-om ili SAX-om manipulirati podacima.
Također može biti da nam treba DTD jer želimo provjeriti valjanost XML-a kojeg imamo. ugl može biti svašta :)

Pol sata nas je pitao CGI u sva tri kruga smo tepli po CGIu i varijacijama na temu, zasto je dobar zasto nije, kako to rjesiti bla bla :) i to je – naglasak na CGI

Primjer klijentskih tehnologija:
XHTML, CSS, JavaScript, DOM

Web 2.0, što je to i kojim tehnologijama se realizira:
Web 2.0 je trend u World Wide Web tehnologiji baziran na socijalizacijskoj noti koja korisnicima omogućava sudjelovanje u kreiranju sadržaja weba

Osnovne karakteristike Web 2.0 su otvorenost, sloboda i kolektivna inteligencija. Korisnici mogu koristiti aplikacije u potpunosti kroz web preglednik – dakle web se definira kao platforma te imaju kontrolu nad podacima na nekoj stranici. Zatim, sama arhitektura Web-a 2.0 potiče korisnike da tijekom korištenja daju svoj prilog nekom Web sadržaju ili aplikaciji. Nadalje su tu neki aspekti društvenog umrežavanja (društveni softveri unutar društvenog networking-a) te kvalitetnije grafičko uređenje nego na Web 1.0.
Društveni networking je postao sinonim za Web 2.0. On označava aktivno sudjelovanje u virtualnim zajednicama tj. skupina korisnika zajedničkih interesa okupljena oko nekog internetskog servisa (blogovi, forumi, itd.). Najpopularniji socijalizacijski webovi (društveni softveri)
su Facebook i MySpace.

DHTML:
Dinamic hypertext markup language – Promjena izgleda - svojstava elemenata stranice
nakon početnog prikazivanja stranice o provjera podataka iz obrazaca prije slanja poslužitelju
o prikazivanje dijelova stranice u ovisnosti o kontekstu o izrada "bogatijeg" sučelja (izbornici, poruke ...) Nije potrebno ponovno učitavanje stranice.

Norme : kakve norme postoje (de facto i de iura - znati objasniti u teoriji kako se koja koristi i kako je koja definirana, korištenje koje je manji ili veći rizik, na primjeru obrazložiti za koju normu biste se odlučili ako morate birati)
Norme može donijeti formalno neovisno **tijelo** (npr. W3C): tada je to pravna norma – de iure lat.
Slijedi vodeću tehnologiju, dobitak na vremenu. primjeri: TCP/IP protokol, ASCII, Unicode, Wireless 801.11n
Tržište donosi također norme, široko prihvaćen proizvod postaje norma - de facto/proizvod, Primjer: IBM PC, tpkovnice QWERTY, modemske naredbe "AT",
Također postoji treća vrsta: široko prihvaćen proizvod **licenciran** drugima - de facto/licenca (licensable), Primjer: AT&T UNIX

Ako uzmemo de facto normu, koja je ustaljena neko vrijeme tada ona može imati mali ali i veliki rizik jer neznamo kako će biti za 5 godina i hoće li se ona pokazati dobrom
Kod pravne je to definirano, zato jer je bio onaj veliki postupak dok dođe do pravne norme.. (primjer za AES algoritam). Zato je sigurna, tj je rizik mali.
to je logično , valjda. kad ovi raspišu natječaj puno se njih prijavi za odabir upravo njene pravne norme.
dok kod proizvoda to je teško napravit i progurat zato je možda mogućnost mala.

Sigurnosni zahtjevi:
Povjerljivost – očuvanje tajnosti poruke samo pošiljatelju i primatelju
Cjelovitost – sadržaj poruke ne smije se mijenjati tokom prijenosa
Izvornost –određivanje autentičnosti pošiljatelja
Neporecivost – nemogućnost poricanja slanja poslane poruke

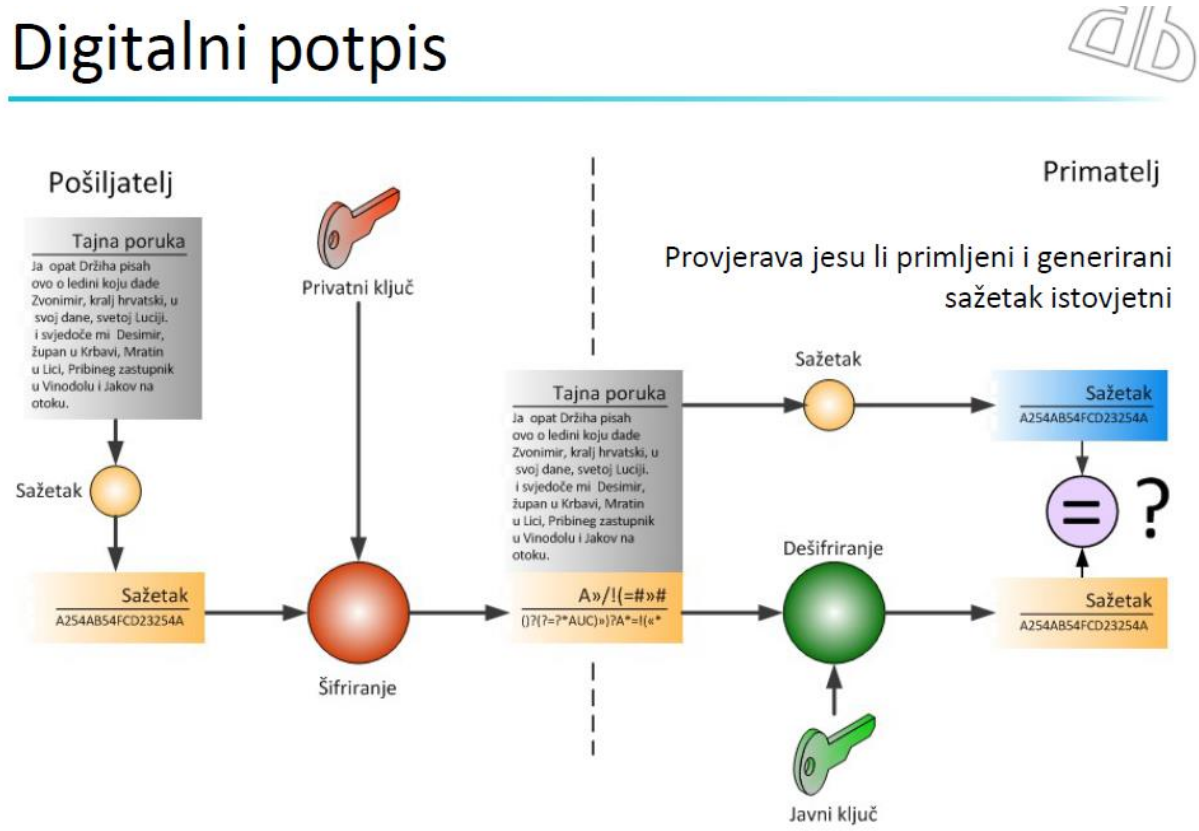
Kriptiranje :
Klasika pitanja - javni i privatni ključ
Javni ključ mogu dobiti svi. Privatni ključ posjeduje samo neki.

Simetrično i asimetrično kriptiranje:
Simetrični algoritmi : isti ključ za kriptiranje i dekriptiranje, sigurnost ovisi o duljini ključa i o mehanizmu dogovora prijenosa ključa između primatelja i pošiljatelja. npr. AES(Rijandel), 3DES algoritmi. Prednosti: brzi, puno algoritma postoji. Mane: distribucija ključa

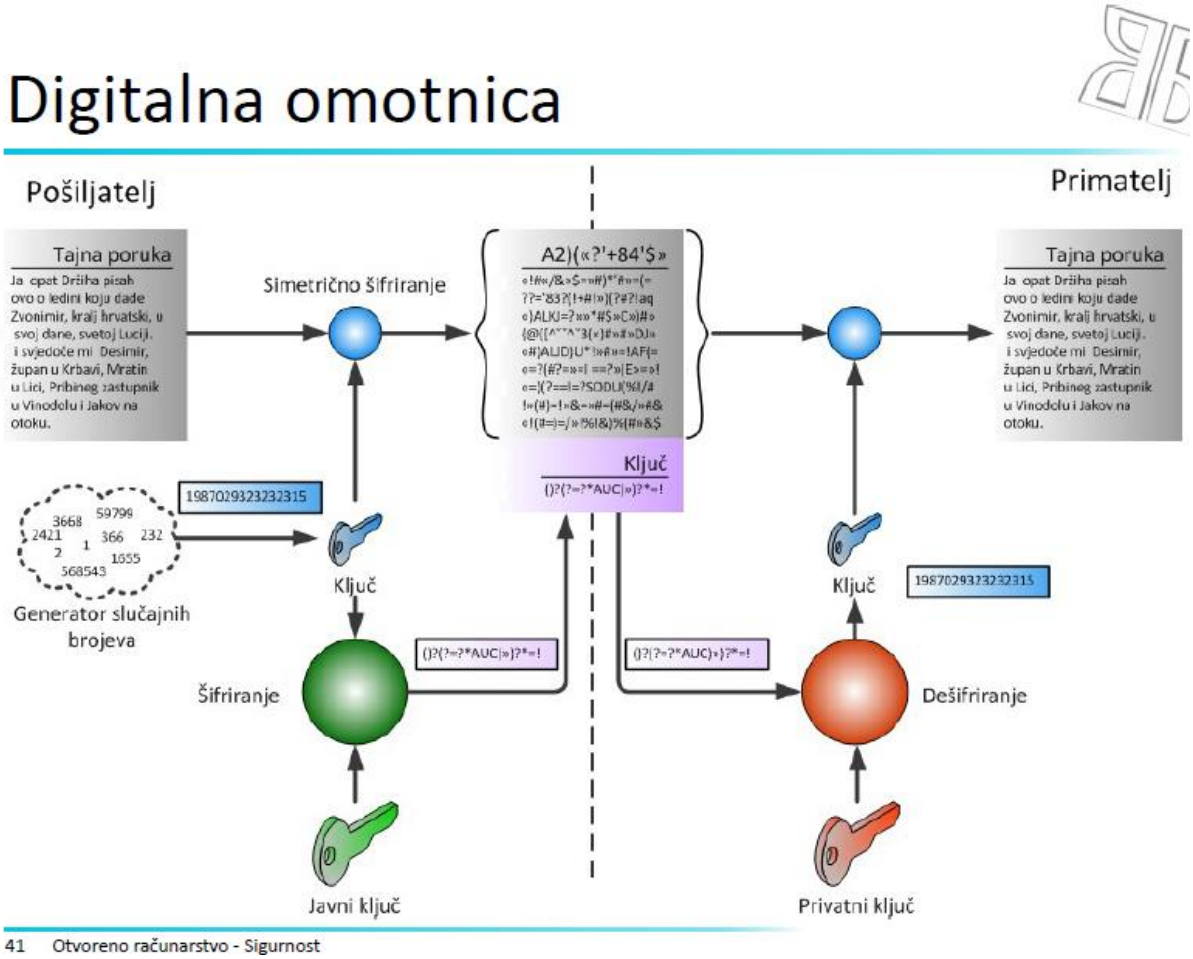
Asimetrično kriptiranje : različiti ključevi za kriptiranje i dekriptiranje. Temeljeni na NP matematičkim teškim problemima. Sigurnost ovisi o odabranom problemu, duljini ključa, zaštiti tog tajnog ključa.
Važno: šifrira se javnim ključem pošiljatelja, dešifrira se tajnim ključem primatelja. (valjda)
Prednosti: distribucija ključeva-pošto je javni, svatko ga može vidjeti i dobiti. Mane: velika računska složenost, sporost.

Digitalni potpis: prednosti i mane:
Princip digitalnog potpisa; Pošiljatelj generira sažetak poruke, Pošiljatelj kriptira sažetak poruke **svojim privatnim ključem**. Pošiljatelj dodaje kriptirani sažetak na poruku. Šalje poruku.

Primatelj javnim ključem dešifrira poruku. Također od izvorne poruke radi sažetak te provjerava jeli tako dobiveni sažetak isti dekriptiranom sažetko poslane poruke.
Ako jest; očuvano je: ovjera izvornosti, cjelovitost, neporecivost



Digitalna omotnica i potpis, postupak verificiranja javnog ključa:
Pošiljatelj generira slučajan broj, te šifrira poruku. Generirani slučajni broj se šifrira javnim ključem te se to dobiveno dodaje šifriranoj poruci. Sve zajedno se šalje kanalom. Na primateljevom strani, prvo se onaj dobiveni šifrirani slučajno generirani ključ dešifrira s privatnim ključem, te ono što dobijemo s time dešifriramo poruku. Eto nadam se da je jasno :D



Čavrak pitanja:

Pitao je o kako teče komunikacija između klijenta i servera:
Klijent s poslužiteljem komunicira protokolom HTTP, hyper text transfer protocol, Klijen šalje zahtjev, a poslužitelj vraća odgovor. Ide redom: HTML, CSS, slike itd. Također prvo ide komunikacija preko DNS servera za dohvat IP adrese iz URIa ako ne postoji još, te potom ide http zahtjev poslužitelju na kojem su smješteni resursi.

URI, URL, URN razlika:
URI – uniformn resource identifier, jedinstveni identifikator resursa. Dijeli se na URL i URN.
URL – uniformn resource locator, URI koji sadrži informaiciju o lokaciji resursa
URN – uniformn resource name, podskup URIa koji sadrži ime resursa

Kako klijent zna kakvu vrstu odgovora će dobiti (MIME):

MIME-multipurpose internet mail extension – za označavanje podataka, označavanje načina kodiranja podataka,struktiruranje poruka. Primjena: elektronička pošta, internetski protokoli. tip/podtip.

Razliku između open source i freeware programa:
Kod freeware programa, programi/aplikacije su slobodni u pogledu skidanja, kopiranja i umnožavanja, ali korisnik nemože dobiti uvid u izvorni kod. Open source programi su kao i freeware samo što dodatno korisnik može vidjeti cijeli izvorni kod programa.