Università degli Studi di Udine

DMIF — Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Esame di **Reti di Calcolatori**

Soluzione

A.A. 2016-17 — IV appello — 17 luglio 2017

1. Al tempo $t_0 = 0$ un'antenna posta sulla terra inizia a inviare con velocità $c = 2.5 \cdot 10^8$ m/s un segnale sinusoidale verso un satellite che si allontana da essa a una velocità costante $c_S = 2.5 \cdot 10^6$ m/s. Si calcoli la frequenza f a cui il segnale dev'essere inviato affinché il satellite riceva un segnale sinusoidale a frequenza $f_S = 10$ MHz.

   R: Poichè la velocità è indipendente dalla lunghezza d'onda $\lambda = c/f$, che resta dunque costante al variare della prima, possiamo eguagliare quest'ultima al ricevitore S e al trasmettitore T ottenendo

   $$\frac{c - c_S}{f_S} = \frac{c}{f_T} \Longrightarrow f_T = \frac{c}{(c - c_S)} f_S = \frac{2.5 \cdot 10^8}{2.5 \cdot 10^8 - 2.5 \cdot 10^6} 10^7 = \frac{10^9}{10^2 - 1} = 10101010.1 \text{ Hz}.$$

2. Si crea un canale giuntando cavi identici attraverso amplificatori non ideali, progettati per restaurare la potenza del segnale al valore che aveva in ingresso al cavo. Ogni cavo attenua la potenza del segnale in ingresso di un fattore $\beta = 3$, e non aggiunge rumore. Ogni amplificatore restaura come detto la potenza, aggiungendo contemporaneamente un rumore di potenza N_0. Detta P_0 la potenza del segnale in ingresso al canale, dopo quante coppie cavo/amplificatore il rapporto segnale/disturbo presente in uscita dalla prima coppia si riduce di 10 dB?

   R: Poiché ogni amplificatore restaura il segnale e aggiunge un rumore di potenza N_0, dopo l'n-esima coppia cavo/amplificatore il rapporto segnale-disturbo vale $\text{SNR}_n = P_0/(nN_0)$. Una riduzione di 10 dB corrisponde a una riduzione dello stesso rapporto di un fattore 10. Dunque, $n = 10$.

3. Detta C la capacità del canale in corrispondenza della prima coppia cavo/amplificatore dell'esercizio precedente, quanto vale la capacità in corrispondenza della coppia avente rapporto segnale/disturbo ridotto di 10 dB se la banda di ogni cavo vale $B = 20$ MHz e se $P_0/N_0 = 10^3$?

   R: $C_{10} = B \log_2(1 + \frac{P_0}{10N_0}) = 20 \cdot 10^6 \log_2(1 + \frac{10^3}{10}) = 20 \cdot 10^6 \log_2(101) = 20 \cdot 6.66$ Mbit/s $= 0.668C$.

4. Si considerino le codifiche di bit NRZ, NRZI e Manchester. Quale delle tre è insensibile a un'inversione di segno della tensione del segnale codificato che dovesse avvenire nel canale all'insaputa del decodificatore? Si spieghi perchè.

   R: NRZI, in quanto la determinazione della costanza o commutazione del segnale non dipendono da una sua eventuale inversione avvenuta nella linea.

5. Una linea di trasmissione di pacchetti di lunghezza $L = 4$ bit ha una probabilità di errore per bit $p = 10^{-6}$. Si assume per semplicità l'indipendenza dell'errore su ciascun bit. In tal caso, si calcoli la probabilità che 3 pacchetti consecutivi contengano in tutto uno e un solo errore.

   R: Se 3 pacchetti consecutivi contengano in tutto uno e un solo errore allora un singolo errore è presente in uno dei 12 bit costituenti i tre pacchetti: $P[\{\text{un errore in 12 bit}\}] = 12p(1-p)^{11} \approx 12 \cdot 10^{-6}$.

6. Si calcoli la moltiplicazione della sequenza `1010101` per la sequenza `101` in aritmetica modulo 2.

   R: Passando alla rappresentazione polinomiale:

   $(x^6 + x^4 + x^2 + 1)(x^2 + 1) = x^8 + x^6 + x^6 + x^4 + x^4 + x^2 + x^2 + 1 = x^8 + 1$, da cui

   `1010101`·`101` = `100000001`.

7. In un cavo Ethernet lungo 800 m convenzionalmente si assume che le informazioni viaggino a $5 \cdot 10^7$ m/s. Qual è la lunghezza minima in bit che deve avere un pacchetto nel caso in cui la Ethernet funzioni a 10 Mbps?

   R: Ricordando che il trasmettitore deve persistere sul canale per un tempo uguale al tempo massimo di andata e ritorno, il numero di bit che garantisce detta persistenza è

   $10^7 \dfrac{2 \cdot 800}{5 \cdot 10^7} = 320.$

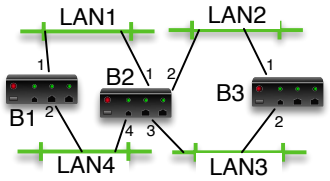
8. Se n è il numero di elementi che costituiscono l'alfabeto di un messaggio da comprimere, quanti saranno gli elementi dell'alfabeto del messaggio compresso nel caso si adotti la codifica RLE?

   R: All'alfabeto di numerosità n occorre aggiungere un numero k di simboli in grado di descrivere il numero di occorrenze consecutive di ciascun carattere che forma il messaggio. Se si adopera una base binaria per esprimere questo numero allora $k = 2$, altrimenti più in generale k è uguale appunto alla base scelta.

9. Quanto deve essere il CIDR x minimo affinché 192.168.160.0/x sia un indirizzo di rete valido? Usando tale CIDR, quante sottoreti di 192.168.0.0/16 verrebbero create?

   R: Convertendo 160 in binario si ottiene 10100000, quindi ci vogliono 8+8+3 bit per coprire fino all'ultimo 1, quindi $x = 19$. Le sottoreti totali sono quindi 8.

10. Nella rete a lato, i bridge si sono configurati secondo l'algoritmo di spanning tree. Un host sulla LAN4 prova a "pingare" gli host A sulla LAN1, B sulla LAN2 e C sulla LAN3, tutti uguali fra di loro. Da quale host avrà i tempi di risposta maggiori, e perché?



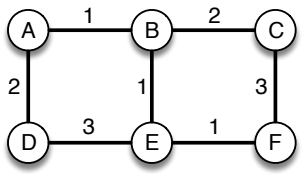
   R: Il root bridge è B1, mentre B3 si disattiva. Quindi i percorsi dalla LAN4 a LAN2 e LAN3 hanno la stessa lunghezza, e quindi i tempi massimi saranno da B e C.

11. Ad un host arrivano i pacchetti IP come nella tabella a lato. A quale istante viene ricostruito il payload e consegnato allo strato superiore? Come viene gestito l'ultimo pacchetto?

istante (ms)	length	offset	MoreFrags
0	800	0	1
10	400	100	1
15	800	100	0
20	400	150	0

   R: All'istante 15ms. Il frammento di quell'istante completa quello ricevuto all'istante 0, sovrapponendosi in parte a quello arrivato all'istante 10. L'ultimo pacchetto viene trattato come se fosse un frammento di un nuovo pacchetto: viene allocato un buffer in attesa degli altri frammenti, ma siccome non arrivano al timeout tale buffer viene deallocato e il frammento cancellato.

12. I router della rete a lato utilizzano un algoritmo di routing basato sullo stato delle linee. (a) Si dia il percorso da A a F, e da D a C, con i rispettivi costi. (b) A causa di un bug, E rileva che il link E-B si è interrotto, mentre B lo vede ancora funzionante. Come cambiano i percorsi da A a F e da D a C?
    R: (a) A-B-E-F, costo 3; D-A-B-C, costo 5. (b) Da A a F non cambia, perché la direzione B-E funziona ancora, o per lo meno così si pensa. Anche da D a C non cambia (e continua a funzionare).



13. Un provider Internet (ISP) locale offre la connessione ad alcuni clienti, e si collega a due provider nazionali. (a) Che tipo di AS è questo ISP (stub, multihomed, transit)? (b) Quali prefissi di rete pubblicizzerà ai suoi provider?

    R: (a) Di transito. (b) I suoi e quelli che gli vengono pubblicizzati dagli speaker dei suoi clienti.

14. Due host si scambiano messaggi da 100 byte l'uno, via UDP. Quanto è l'overhead (ossia il traffico aggiuntivo) dovuto alle intestazioni di trasporto e di rete, in percentuale? E con payload di 1000 byte?

    R: L'intestazione IP è di 20 byte, quella UDP è di 8, quindi in totale l'overhead è $28/128 = 21,9\%$. Nel caso di payload di 1000 byte, è $28/1028 = 2,72\%$

15. Durante la fase di handshake di una connessione TCP, il server (ossia l'entità che ha eseguito l'apertura passiva) ha inviato il SYN+ACK ma il corrispondente ACK dal client (i.e., quello che ha eseguito l'apertura attiva) al server è andato perduto. Il client può iniziare a spedire dati lo stesso? E il server?

    R: Sì, il client si trova in stato ESTABLISHED e può iniziare a mandare dati. Se l'ACK dal client era perduto, uno dei nuovi segmenti ne farà le stesse funzioni. Invece il server no, deve aspettare un ACK per spostarsi in ESTABLISHED.

16. Una entità ha appena ricevuto un segmento con `Acknowledged`=13000, `AdvertisedWindow`=4000. Se il buffer di invio è grande 5000 byte, e `LastByteWritten`=16000, qual è la quantità minima di dati che l'applicazione può ancora scrivere sulla socket prima di bloccarsi?

    R: La quantità minima è quando l'applicazione destinataria non consuma niente. Nel buffer di invio ci sono attualmente 3000 byte da inviare o inviati e non riconosciuti, quelli che vanno da 13000 a 15999. Però nel buffer di ingresso del destinatario ci sono ancora 4000 byte di spazio a partire dalla posizione 13000, quindi possiamo trasferire tutti i 3000 byte attualmente in coda più altri 1000, prima che il buffer di ingresso del destinatario si riempia. A quel punto abbiamo ancora l'intero buffer da 5000 byte da riempire. In totale, l'applicazione può scrivere 1000+5000=6000 byte.

17. Un router sta servendo tre flussi A, B, C, secondo la politica di accodamento equo (Fair Queueing). I pacchetti inizialmente in coda, con il tempo necessario per trasmetterli (in ms), sono i seguenti: A1=100, A2=100, B1=200, B2=100. All'istante 50 arriva un pacchetto C1 di lunghezza 200. A che istante inizia la trasmissione di B2?

    R: Secondo FQ, l'ordine di conclusione di invio dei pacchetti è: A1=100, A2=200, B1=200, B2=300, C1=250. Quindi l'ordine di trasmissione è A1, B1, A2, C1, B2. Sommando i tempi, B2 inizia a 600.

18. Si diano almeno due motivi per cui i protocollo di sicurezza wireless (come WEP, WPA, WPA2) si basano su cifratura simmetrica.

    R: (2pt) Essenzialmente, per efficienza e semplicità (e quindi minori costi). Per semplicità implementativa: è sufficiente avere una chiave condivisa tra tutti i nodi della cella wireless, e non è necessario distribuire chiavi pubbliche/private. Per efficienza: dato che devono essere implementate all'interno della scheda wireless, la cifratura simmetrica è molto più facile da implementare in hardware o firmware di processori non troppo potenti. Infine, per parallelismo con la rete Ethernet cablata: usare una unica chiave simmetrica condivisa tra tutti i nodi della cella equivale a creare una LAN cablata condivisa.

19. Sarebbe indicato un cifrario a flusso, come RC4 o un cifrario a blocchi in modo OFB, per cifrare un file ad accesso casuale (ossia con la possibilità di accedere in lettura o scrittura in qualsiasi punto del file)? Dove si memorizzerebbe il vettore di inizializzazione?

    R: No, perché ogni volta che si accede al file, bisognerebbe iniziare a generare il keystream dall'inizio, che è molto pesante. Meglio utilizzare un altro modo (CBC o CTR). Se proprio si vuole usare un cifrario a flusso, meglio segmentare il file in blocchi di qualche kB, da cifrare separatamente. Il IV si può memorizzare assieme al file o ai blocchi, non cifrato (non è una informazione segreta).

20. Alice si fa rilasciare un certificato X.509 da una certa CA. Dopo alcuni giorni, si scopre che la CA è stata colpita da un attacco hacker che ha portato alla compromissione della chiave privata usata per firmare i certificati. La chiave privata dell'utente è a rischio? E la validità del certificato?

    R: No, la chiave privata di Alice rimane segreta, quindi non è a rischio. Però non possiamo essere sicuri se il certificato sia stato rilasciato dalla CA o da un attaccante; non solo, l'attaccante potrebbe perfino generare altri certificati associando all'identità di A un'altra chiave pubblica, di cui egli conosce la corrispondente chiave privata; così le controparti potrebbero mandare a A dei messaggi che l'attaccante potrebbe leggere, o l'attaccante potrebbe autenticarsi per A.

    In pratica, quella chiave rubata viene ritirata (ossia, la CA di livello superiore emette una revoca per la chiave della CA rubata), e tutti i certificati firmati con quella chiave vengono ritirati a loro volta. Gli utenti, come Alice, possono farsi emettere il certificato per la chiave che hanno già, da un'altra CA o dalla stessa CA ma dopo che questa ha avuto un nuovo certificato.

21. Nel protocollo a lato, A e B condividono la chiave simmetrica K, N è una nonce generata sul momento da A, H una funzione di hash. Il messaggio M è autentico? È puntuale? È non ripudiabile da A?

    1. $A \to B : M$
    2. $B \to A : E_K(N)$
    3. $A \to B : N, H(K, M)$.

    R: È autentico, ma non puntuale né non ripudiabile.

22. Nel protocollo a lato, A e B conoscono le rispettive chiavi pubbliche, K è una chiave di sessione generata sul momento da B, e M è il messaggio. A è autenticato per B? E viceversa? Perché?

    1. $A \to B : A, E_{PU_B}(E_{PR_A}(K))$
    2. $B \to A : E_K(M)$.

    R: A è autenticato al passo 1., perché firma con la propria chiave privata. B al passo 2, perché risponde all'implicita challenge di ottenere la chiave K.

23. Alice invia a Bob una mail PGP firmata con la sua chiave privata ma NON cifrata. (a) Bob può togliere la firma di Alice, firmare il messaggio con la propria chiave privata, e inviare tutto a Charlie? (b) E se il messaggio che Alice invia a Bob fosse anche cifrato, ma per Charlie?

    R: (a) Sì. (b) Non potrebbe più sostituirsi per Alice: al massimo potrebbe firmare il messaggio "a busta chiusa".

24. Adelmo, dal suo calcolatore A, vuole collegarsi ad un certo sito X, che però sta oltre un router-firewall che elimina tutti i pacchetti indirizzati a X. Adelmo conosce Berengario, il cui calcolatore B sta oltre il router-firewall. Come può Adelmo aggirare l'ostacolo, eventualmente chiedendo aiuto a Berengario?

    R: Creando un tunnel IPSec (ESP o AH, è indifferente) in modalità tunnel, tra A e B. Così i pacchetti uscenti da A vengono recapitati a B, attraversando indenni il firewall perché hanno come indirizzo IP esterno quello di B. Poi B estrae il pacchetto IP interno e lo inoltra a X, che quindi pensa di ricevere il pacchetto da X (in effetti è così, in quanto B funge solo da router). I pacchetti di ritorno possono attraversare il firewall, in quanto sono in uscita.