

תרגיל בית תיאורטי מס' 4

להגשה עד 28.1.2013

TCP Reliable Data Transfer

1) (taken from Kurose & Ross, 5th ed.)

Consider transferring an enormous file of L bytes from A to B.

- What is the maximum value of L such that TCP sequence numbers are not exhausted? Recall that TCP sequence number field has 4 bytes.
- For the L you obtain in (a), find how long it takes to transmit the file. Assume that a total of 66 bytes of transport, network, and datalink headers are added to each segment before the resulting packet is sent out over a 10Mbps link. Ignore flow and congestion control, so A can send the segments back to back continuously. Assume the maximal packet size (including headers of all layers) is 1514 bytes.

RSA

(2) נתונים המספרים הראשוניים $p = 7, q = 13$.

- מצאו מפתח פומבי ומפתח פרטי מתאימים.
- השתמשו במפתח הפומבי כדי להצפין ב-RSA את ההודעה $m = \text{"RSA"}$, מקודדת ב-ASCII. הצפינו כל אות בנפרד. שימו לב שתצטרכו לערוך חישובים מדוייקים על מספרים שלמים גדולים. ניתן לעשות זאת למשל באמצעות BigInteger של Java או C#. תוכלו להשתמש בכל כלי שתבחרו, אך פרטו את כל החישובים שביצעתם.
- השתמשו במפתח הפרטי כדי לפענח את ההודעה המוצפנת.
- האם התהליך היה עובד לו הייתם מצפינים במפתח הפרטי ופותחים במפתח הפומבי? האם יש הגיון לעשות כזה דבר לצורך כלשהו? (רמז: תראו שימוש כזה בהרצאה על Network Security).

P2P

3) (taken from Peterson & Davie, 5th ed.)

Consider the following simplified BitTorrent scenario: There is a swarm of 2^n peers, and, during the time in question, no peers join or leave the swarm. It takes a peer 1 unit of time to upload or download a piece, during which time it can only do one or the other. Initially, one peer has the whole file and the others have nothing.

רשתות תקשורת מחשבים, סמסטר א' 2012/13
ביה"ס למדעי המחשב, אוניברסיטת ת"א

- a) Show that, if the swarm's target file consists of only 1 piece, all peers could have the file after n time units. Ignore all but upload/download time.
- b) Now suppose the target file consists of 2 pieces. Show all the peers could obtain the file in $n + 2$ time units.

Note: It can be shown (and you could take it as a challenge) that in case (b) the file cannot be distributed to all peers in less than $n + 2$ time units.

DNS

- 4) (taken from Peterson & Davie, 5th ed.)
ARP and DNS both depend on caches; ARP cache entry lifetimes are typically 10 minutes, while DNS cache lifetimes are on the order of days.
 - a) Justify this difference.
 - b) What undesirable consequences might there be in having too long a DNS cache entry lifetime? How do these consequences complicate the process of changing the IP address of a web server?
 - c) How can these consequences be minimized? (Hint: DNS records contain a TTL value, specified by the DNS server, representing how long a DNS record may be kept in the client cache).