Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets if necessary.

Total Marks: **30**

[10] 1. (a) Explain the concept of a *certificate chain*; make sure you mention *root certificates* and *target certificates*.

(b) When signing certificates, what is the difference between an *issuer* and a *subject*?

(c) What are the four components of the public key infrastructure?

Solution: A chain of certificates is a sequence of certificates, usually contained in the same file, where one certificate signs the next. The first certificate in the chain is the root, while the last is the target. If Ted signs Carol's certificate, in effect vouching for Carol, Ted is the issuer while Carol is the subject. The four components of a PKI are the following: the certificates issued by a certification authority (CA), a repository for retrieving certificates, a method for revoking certificates, as well as a method for evaluating a chain of certificates from roots (also known as trust anchors).

[10] 2. Fill out the five details of the Kerberos protocol:

(a) A chooses r_A at random and sends (A, B, r_A) to T

(b) T generates new session key k, creates ticket

$$t := (A, k, l) \quad l \text{ is a "validity period"}$$

T sends (_____, _____) to A.

(c) A recovers (k, r_A, l, B) and verifies it matches what was sent in 1.
A creates an authenticator $a := (A, t_A)$ where t_A is A's clock's time-stamp and sends (_____, _____) to B.

(d) B recovers t and a and checks:

i. A is the same in t (ticket) and a (auth.)

ii. t_A (time-stamp) is "fresh" and falls within l

At this point B's authentication of A is successful.

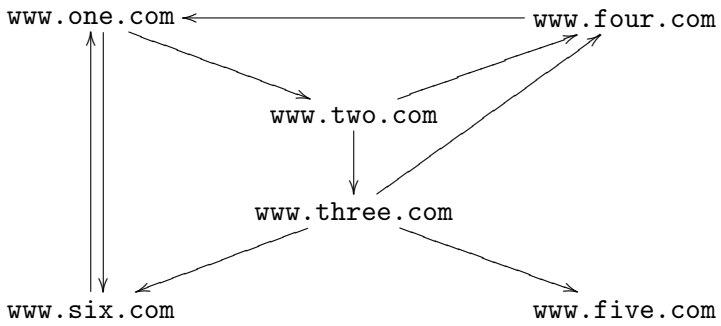
(e) B sends _____ to A

(f) A recovers t_A and checks if it matches what was sent in 3.
At this point A's authentication of B is successful.

Solution: In order, here are the answers:

$E_{k_A}(k, r_A, l, B)$
$E_{k_B}(t)$
$E_k(a)$
$E_{k_B}(t)$
$E_k(t_A)$

3. Consider the following mini-WWW:



The arrows denote links.

(a) Construct the "Google" matrix $G = (g_{ij})$ of this mini-WWW.

(b) From G we construct the matrix $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} d\dfrac{g_{ij}}{c_j} + \dfrac{1-d}{n} & c_j \neq 0 \\ \dfrac{1}{n} & c_j = 0 \end{cases}$$

where d is the "damping factor"—explain what that is. c_j is the sum of the row; what is its purpose? How is A used to compute the ranking of the pages?

Solution:

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

In our case, $n = 6$. $d = 0.85$ is the probability that a "random surfer" stays on the current web page, while $1 - d$ is the probability that the "random surfer" jumps to a random page. $c_1 = 2, c_2 = 2, c_3 = 3, c_4 = 1, c_5 = 0, c_6 = 1$ is used to normalize the columns of the matrix, and hence obtain a stochastic matrix of probabilities. Once A is computed, for (practically) any initial vector x, say $x = (1/6, 1/6, 1/6, 1/6, 1/6, 1/6)$, $A^n x$ converges to the probability that a "random surver" ends up at a particular page. This is then used for the ranking.