Name _____ Student No. _____

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

Total Marks: **30**

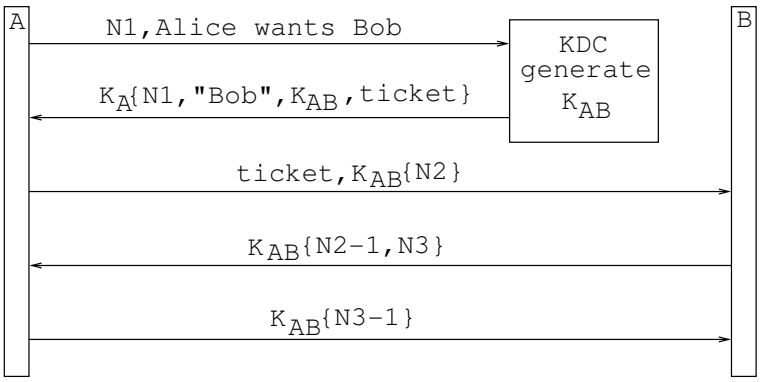
[10] 1. In their paper *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, the founders of Google, Sergey Brin and Lawrence Page, propose the page rank formula:

$$\mathrm{PR}(A) = (1-d) + d\left[\frac{\mathrm{PR}(T_1)}{\mathrm{C}(T_1)} + \frac{\mathrm{PR}(T_2)}{\mathrm{C}(T_2)} + \cdots + \frac{\mathrm{PR}(T_n)}{\mathrm{C}(T_n)}\right].$$

Explain this formula.

Solution: First the terms: $\mathrm{PR}(A)$ is the Page Rank of web page A — the higher the rank, the more "valuable" the page. The parameter d is the "damping factor," usually set to be 0.85 and intended to be the probability of a random surfer staying on the current page. $\mathrm{C}(X)$ is the number of distinct links that leave page; $T_1, T_2, \ldots, T_n$ are the pages that link to page A. In turns out that $\mathrm{PR}(A)$ can be computed (from practically any initial value) by an iterative algorithms that always converges to the principal eigenvector of the normalized link matrix of the web.

[10] 2. Consider the Needham-Schroeder protocol:



(a) What is the "ticket"?

(b) $N_1, N-2$ are called *nonces*; what is their role?

(c) Why do we send one way N_2 but return $N_2 - 1$?

(d) Why is "Bob" included in the second exchange?

Solution: The ticket is $K_{\mathrm{B}}\{K_{AB}, \text{“Alice”}\}$. The role of the nonces is to provide a "challenge-response" mechanism (to assure the players that they are talking to the entity they intended to talk to); if the nonces were returned as they arrived, that would offer no proof of being in possession of K_{AB} — it is being in possession of K_{AB} that offers the proof of authenticity. (Technically, N_3 would not have to be modified, if we used cipher-block chaining in step 4.) In the second exchange, Bob's name is given in case Eve was impersonating Alice to gain a ticket to talk to Bob. This way, Alice would find out that someone was impersonating her to gain access to Bob.

[10] 3. Suppose that you want to login into your Facebook account. Your browser downloads Facebook's SSL certificate; once it has it, what does it do with it? Define and mention *trust anchor*, *chain*, *authenticate*, *issuer* and *subject*.

Solution: In order for your browser to trust the certificate, it has to find a CA that vouches for it; say the CA vouching for Facebook's certificate is VeriSign. Then, VeriSign is the trust anchor (a.k.a., the root). The server provides a chain of certificates from VeriSign to Facebook's certificate. The links in the chain are of the form $[N$'s public key is $n]_x$; at the beginning of the chain is the Root certificate, which is self-signed; then the Root signs the next certificate claiming that Y's public key is y; then Y signs the next certificate claiming that X's public key is x, etc. In the last case, the subject is X and the issuer is Y. The browser has a collection of Root certificates and once such a chain is provided for a particular server's certificate, this server is deemed authenticated.