Cryptography

Description

Prepare a short research paper of approximately 5 pages, double-spaced, exclusive of cover, title page, table of contents, endnotes and bibliography.  Your paper must use APA formatting with the exception that tables and figures (if used) can be inserted at the appropriate location rather than added at the end.  Submit the paper in your assignment folder as a Word attachment with the following file name: yourlastnameSSB.doc   For example, a submission file would be called JonesSSB.doc   Alice, a high net worth customer, banks on-line at Super Secure Bank (SSB) and has agreed to use 3DES in communicating with SSB. One day, Alice received a statement that shows a debit of $1,000,000 from her account. On inquiring, she was told that the bank manager, Bob, transferred the money out of Alice's account and into an account of his own in an offshore bank. When reached via long distance in the Cayman Islands, Bob produced a message from Alice, properly encrypted with the agreed upon 3DES keys, saying: "Thanks for your many years of fine service, Bob. Please transfer $1,000,000 from my account to yours as a token of my esteem and appreciation. Signed, Alice."   Alice filed suit against Bob, SSB and the government of the Cayman Islands, claiming that the message was a forgery, sent by Bob himself and asking for triple damages for pain and suffering.  Bob has responded by claiming that all procedures were followed properly and that Alice is filing a nuisance suit. You have been employed by SSB as a cryptographic expert to assist in the investigation of this matter, and will produce a report for the SSB Board of Directors, which will assist them in determining how to proceed in this matter. Your report to the Board of Directors should address the following issues: ·       What can be determined from the facts as presented about whether Alice intended to make Bob a gift of $1,000,000? ·       Assuming SSB wishes to continue using only 3DES as its cryptographic system, what could SSB and Alice have done to protect against this controversy arising? ·       Would this controversy have arisen if SSB had been using AES rather than 3DES?   Your report should clearly address these issues, with sufficient detail and background to allow the “cryptographically challenged” Board of Directors to understand the issues involved and formulate plans for how to approach the immediate issue with Alice, and to continue business in the future, assuming that they want to continue using 3DES. Please Note: It is not required in this paper to provide a detailed explanation of the 3DES encryption algorithm.

Order 1556131