

Name:
State all assumptions necessary to answer the questions.

CS 585 Test 4
Apr. 11, 2005

Use the first five letters of your last name as a key and encode the word “jugglers” using either the Playfair or ADFGVX ciphers.

Is the ADFGVX cipher an example of a Feistel cipher? Explain.

How does a symmetric key cipher provide authentication?

Name:
State all assumptions necessary to answer the questions.

CS 585 Test 4
Apr. 11, 2005

Which variant of DES, Triple DES or DES-X is backwards compatible with DES? Explain how it is achieved.

Could you substitute in the Hill cipher for the DES function in the DES protocol. If possible explain the effect, if not possible explain why not.

Give an example of a substitution cipher and demonstrate how it works. (Make sure the cipher has no permutation component.)