

Name:
State all assumptions necessary to answer the questions.

CS 585 Final
May 4, 2005

Suppose you are given a function f that maps short integers (2 byte) to 8 bit ASCII characters. You are told that the function has the strong collision property, and that you are to use it for a digital signature. Explain why or why not the strong collision property is useful for this purpose.

Why is it important to use prime numbers for generating the keys in RSA?

Consider users A and B, and the RSA public key (e, n) and private key d . Suppose that both A and B (and only A and B) had both keys and that to communicate they would encrypt using the private key and decrypt with the public key. Why or why not is this still an asymmetric cipher? What other considerations are there if RSA is used in this manner?

Name:
State all assumptions necessary to answer the questions.

CS 585 Final
May 4, 2005

What is the Diffie-Hellman protocol used for? What are the trade-offs involved in using it?

In the setup of the MASH-2 algorithm, two primes are chosen and used to compute a value M . What is M used for?

Would it be practical to use RSA as a message digest technology in place of MASH-2? Conversely would it be practical to use MASH-2 for message encryption in place of RSA? Explain.