Name ______________________.

Plgwhup Hadp

HHFV 598-1
Fubswrjudskb dqg Qhwzrun Vhfxulwb

Iheuxdub 21, 2001

1. Consider a linear congruential generator $X_{n+1} = (aX_n + c) \bmod m$.

   Are the parameters a = 314,159, c = 5, and m = 1,000,000 good choices?

2. In a trusted third party key distribution session, Alice requests a session key from the key distribution center. The KDC distributes a session key to Alice encrypted under her key, and a copy of the session key encrypted under Bob's key.

   After Alice sends Bob the session key, Alice and Bob each send one more message. Describe these two messages and explain why they are necessary.

3. Alice and Bob share a secret DES key. Their communication is required to be authenticated but not confidential. Along with each message, Alice and Bob are allowed to send one additional eight byte authenticator.

   How can Alice use DES cipher block chaining to authenticate their messages? Assume the initialization vector is 0.

4. What is the essential difference between DES Output Feedback Mode and Cipher Feedback Mode?

5. Rijndael uses arithmetic in GF(2^8). Give two reasons why x^4 is a bad choice for the reducing polynomial.

6. Explain why the round function in a classic Feistel network need not be reversible. Draw a picture if you think will help convince me.

7. Give two reasons why Blowfish does not use static S-boxes.

8. Why does Triple-DES hardware usually implement EDE mode?

Li brx fdq uhdg wklv, wkhq brx pxvw eh grqh zlwk wkh hadp, vr brx pdb jr.