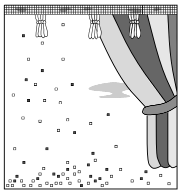
April 20, 2000

Crypto review for the final exam

Exam conditions Again, the final exam will be "open book, open notes". You may bring to the exam anything additional to help you which is *non-living*.

Define, explain, or briefly discuss each of the terms below.
1. Enigma 2. VENONA 3. DES 4. One time pad 5. Depth 6. "Randomness" 7. Binary 8. The discrete log problem 9. Polynomial time algorithm 10. Exponential time algorithm 11. Encryption 12. Encryption key 13. Decryption key 14. Hash 15. Algorithm 16. Man in the middle attack 17. Certificate authority 18. Plain text 19. Cipher text 20. Secret Sharing 21. Steganography 22. One-way function 23. Factoring and cryptanalysis 24. Trapdoor in a cryptosystem 25. Pseudo-random 26. Collision (hashing) 27. Public key encryption 28. Exhaustive search



A. Our messages are positive integers, such as **2**3278**7**. A hashing algorithm is applied to these messages. The result is the product of the first and last digits of the message. Since $2 \cdot 7 = 14$, 14 is the hash value of the message 232787. Are collisions possible? If they are, exhibit two messages with the same hash. Can 43 be a hash value for some message? Estimate how many distinct messages there could be whose hashes are all different.

B. John receives the message, "Darling, I love you!", supposedly from Gilda. Describe a crypto environment in which he can be reasonably certain that the message was actually from Gilda.

C. A committee of seven people wish to share a secret (which can be thought of as a number!) so that any majority of the committee (at least four members) must agree to have access to the secret. Describe how to do this. Illustrate your description with a worked-out example. (Simple examples are fine!)

D. There are many cell phones in western Europe*. Describe a reasonable strategy by which two cell phones, after being connected by the network, could "negotiate" and then transport a long conversation with some likelihood of privacy. Due to the size of cell phones, the dynamics of the market, and the structure of the network, it is not reasonable to suppose that every individual cell phone can carry information about every other individual cell phone.

E. On what basis do people decide whether or not an encryption system is secure? Explain your answer.

F. The only words in a language are **A**= 111 and **B**= 0000. Two sentences in the language are xor'd with the same random bitstream, and we observe:

First sentence flipped : 01110 11010 01000 11100 1;
Second sentence flipped : 01101 01101 10100 11111 0.

Use this information to find good candidates for the original sentences.

* Many more, per capita, than in the U. S.