

Things to review for the 103h Final

Instructor: Wesley Pegden

Everything from the first midterm!

This will be a little under half the exam. . . 30-40%.

The perfect code system

Question 1. Describe in a paragraph or so precisely how the perfect code encryption system works.

Question 2. What ‘hard problem’ does the perfect code system depend on?

Number Theory

Question 3. Find $\gcd(493, 667)$ using the Euclidean algorithm.

Question 4. Find $\gcd(1219, 1537)$ using the Euclidean algorithm.

Question 5. Find the inverse of 132 mod 195 using the Extended Euclidean algorithm.

Question 6. Find the inverse of 232 mod 439 using the Extended Euclidean algorithm.

Question 7. Find $13^{29} \pmod{53}$

Question 8. Find $15^{32} \pmod{79}$

Question 9. State Fermat’s little Theorem, and describe how it can be used to find large prime numbers for RSA. (Explaining this may take a paragraph or more. I would recommend that you actually try writing it down.)

RSA

Question 10. If Alice wants to send Bob a message encrypted with RSA, who needs to generate an RSA keypair?

Question 11. You want generate an RSA keypair. You have choose $p = 13$, $q = 7$, and $e = 5$. What is your public key? What is your private key?

Question 12. Continuing the above example, if I send you the ciphertext 61, what does that decrypt to? My public key is $(7, 91)$. Do you need to know it to answer this question?

Question 13. You are trying to send me the message MATH ROCKS. First, encrypt this message using the Caesar cipher with the key 6. Next, encrypt the key to send to me using RSA; I have published the public key (7,91).

Question 14. Explain why, in practice, RSA is used to transmit the keys for a block cipher rather than the message itself.

Question 15. What is the ‘hard problem’ RSA is based on?

Digital signatures and hash functions

Question 16. If Alice wants to sign a message to Bob, who needs to generate an RSA keypair? Explain how the keypair will be used to sign the message and check the signature.

Question 17. If Alice wants to sign and encrypt a message to Bob, who needs to generate an RSA keypair?

Question 18. Alice wants to send the message 10 to Bob and send a signature for it. Alice’s public key is (11,91) and her private key is (59,91). Bob’s public key is (23,77) and his private key is (47,77). (Note, you may not need all of these keys to do this problem!). What does Alice send to Bob?

Question 19. What is a hash function?

Question 20. Explain why hash functions are used when signing messages with RSA.

Question 21. Alice wants to send the message “IM COMING BACK” to Bob and send a signature for it. Alice and Bob have agreed to use the ‘ToyHash’ algorithm to for signatures. Alice’s public key is (11,91) and her private key is (59,91). Bob’s public key is (23,77) and his private key is (47,77). What does Alice send to Bob? (The ToyHash formula is $v^2 + cv + w \pmod{19}$.)

Steganography

Question 22. What is steganography? (This should take about a paragraph to clearly state—what are the goals as opposed to encryption, etc.)