Name_____

CMSCI 358 Exam 1 (Due 9/25/20)

Directions: This is a take-home test. Take as much time as you need for test, as long as it is in by the due date. You may use any resources you like as long as they don't involve another human helping you. For instance, you can use books, class notes, websites, and calculators. But you must not get assistance in any form from anyone in class, any professor, any family member, anybody on the internet, etc. The only exception is you can ask me for clarifications on what a problem is asking.

You can either do your work on the test itself or on a separate sheet. Be sure to show all work.

1. Please write or type a statement in your own words saying that you did not receive assistance on this test, that you did not give anyone assistance, and that this is 100% your own work. **This problem is not optional.**

2. True or False.

   (a) _____ Hash functions are often used to tell if a file's contents have been changed.

   (b) _____ The problem with using hashing as an encryption method is that it would be not be possible to decrypt the hash.

   (c) _____ Suppose we encipher some text by generating a key that is the same length as the message and truly random. We also destroy the key immediately after using it. Then the cipher is mathematically unbreakable.

   (d) _____ 140-bits is currently considered a safe level of security for ciphers.

   (e) _____ The linear congruential PRNG used in the Java programming language is considered cryptographically secure.

   (f) _____ The security of Diffie-Hellman relies on the fact that it is very hard to reverse the mathematical operation (modular exponentiation) that is used in the process.

   (g) _____ One weakness of MD5 is that the hash length can vary based on how long the input data is.

   (h) _____ If you change one bit of an input to the SHA-256 hash function, the hash will almost certainly change considerably.

   (i) _____ The prime numbers used in RSA and Diffie-Hellman need to be many hundreds of digits long in order to be secure.

   (j) _____ Using a 16-bit counter in CTR mode is a bad idea because it will wrap around after 65,536 blocks and cause keystream reuse.

3. Order these ciphers from 1 (least secure) to 5 (most secure). All 5 numbers should be used.

   ___ AES ___ One-time pad ___ Playfair ___ Substitution ___ DES

4. Order these ciphers from 1 (least secure) to 3 (most secure). All 3 numbers should be used.

   ___ CBC ___ ECB ___ GCM

5. Order these hash functions from 1 (least secure) to 3 (most secure). All 3 numbers should be used.

   ___ MD5 ___ SHA-1 ___ SHA-2

6. The fact that certain letters appear more often than others in English text has been extremely useful in breaking which of the following ciphers? Choose all that apply.

   (a) AES (b) DES (c) Substitution (d) Vigenère

7. For which of the following ciphers is it feasible for an attacker with a few thousand dollars of computing power to brute-force try all possible keys? Choose all that apply.

   (a) 2048-bit RSA (b) AES (c) Columnar transposition (d) DES (e) Substitution

8. Which of the following are types of public key cryptography? Choose all that apply.

   (a) AES (b) DES (c) Playfair (d) RSA (e) Salsa20

9. One of my browser's ciphersuites is `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`. Which specific part of it corresponds to the process by which Alice and Bob derive keys to use for encryption?

   (a) CHACHA20 (b) ECDHE (c) POLY1305 (d) RSA (e) SHA256

10. Suppose plaintexts P_1 and P_2 are encrypted with a stream cipher to produce ciphertexts C_1 and C_2. The same keystream was used to encrypt both. What will be the most likely result of $C_1 \oplus C_2$?

    (a) A totally jumbled mess with no parts of P_1 or P_2 discernable.
    (b) Some parts of P_1 and P_2 discernible, while other parts are jumbled together.
    (c) The complete contents of either P_1 or P_2, but none of the other.
    (d) The complete contents of both P_1 and P_2.

11. Which of these are we allowed to reuse for different encryptions?

    (a) The CBC IV
    (b) The CTR nonce
    (c) RSA public/private key pair
    (d) All of the above
    (e) None of the above

12. The primary use of RSA in modern TLS is

    (a) encrypting large files
    (b) digital signatures
    (c) message authentication codes
    (d) all of the above
    (e) only b and c

13. If Alice generates a public/private key pair, how do we know the key really is Alice's?

    (a) She gets a certificate for it.
    (b) We look up her private key in the Root CA's online public key repository.
    (c) Alice digitally signs a document with it, so we know it's hers.
    (d) Alice encrypts a random number with her private key and we verify it with the public key.

14. If we replace the true random number generator of a binary one-time pad with a pseudorandom number generator, what is the name for the type of cipher we obtain?

15. The general terms for a mathematical operation that is simple to perform but challenging to undo is what? This type of operation is important in modern cryptography.

16. Alice generates a public/private key pair. She then takes a message, hashes it, and encrypts the hash with her private key. Various other people decrypt it and see if the result matches the hash of the message. This is a description of what very specific concept that we covered in class?

17. When software developers program RSA, they need to do something to make sure that the exponentiation process takes the same amount of time regardless of the binary structure of the private key. This is needed in order to stop what specific class of attacks?

18. Alice and Bob exchange the number 449 ahead of time. Alice is sending the message "hello". She also computes `x=SHA('hello449')` and sends that to Bob along with the encrypted message. What is `x` called? There's a very specific term for it.

19. If we can break a 32-bit security for a certain cryptosystem in 30 seconds on a laptop, how much time would be required if some parameters are tweaked to bring it up to 36-bit security?

20. Burke96 is a new 96-bit hash function. About how many things do we have to hash before it becomes likely that some pair of them will end up having the same hash?

21. The inhabitants of central Greenland use an alphabet whose 10 characters are the following: `AB$?ZN&"\8`.

    (a) Encrypt the 6-character message `A?ZA?"` using a substitution cipher with key `B$N&8"\Z?A`

    (b) Use the Vigenère cipher with key `AB?N` to encrypt the 7-character message `&Z?8BN8`.

22. Use columnar transposition to encrypt the message `CRYPTOGRAPHY`, with three columns using the key $(2, 1, 3)$. You must show all your work on this. Answers without sufficient work will receive no credit.

23. Write out the 5 × 5 Playfair table for the key REPEATER. Follow the same conventions as in class.

24. Use the Playfair cipher with the 5 × 5 table below to encrypt the message FALLISHERE. Follow the same conventions as in class.

C	H	E	R	Y
T	A	B	D	F
G	I	K	L	M
N	O	P	Q	S
U	V	W	X	Z

25. Encrypt the message 00110101 with a stream cipher whose keystream is 10110111.

26. A stream cipher has been used to encrypt two messages with the same keystream. Plaintext 11101 has been encrypted into 00101. Some unknown plaintext has been encrypted into 10110. What is this unknown plaintext?

27. This problem involves encrypting with a block cipher. The encryption process we will use is simply to reverse the order of the bits in the block. For instance, the 8-bit block 11100010 would get encrypted (reversed) into 01000111.

(a) Assuming 4-bit blocks, encrypt 000110001010 in ECB mode.

(b) Assuming 4-bit blocks and an IV of 1100, encrypt 000110001010 in CBC mode.

(c) Assuming 8-bit blocks, a 5-bit nonce 11011 and a 3-bit counter starting at 0, encrypt 10101010 11110000 00110011 in CTR mode.

28. For RSA, Alice uses $p = 79$, $q = 97$, $e = 5$, and $d = 4493$. You can use Python to do the calculations.

    (a) Encrypt the message $M = 104$.

    (b) Decrypt the message $C = 261$.

29. Alice and Bob do a Diffie-Hellman key exchange. They agree to use the prime $p = 773$ and generator $g = 3$. Alice chooses the random number $a = 111$ and Bob chooses the random number $b = 44$. You can use Python to do the calculations.

    (a) What are the values that Alice and Bob send to each other? Please compute them.

    (b) What is the shared secret? Please compute it.