1. Consider the Vigenere cipher over the lowercase English alphabet, where the key length can be anything from 8 to 12 characters. What is the size of the key space for this scheme?
    a. **26^8 + 26^9 + 26^10 + 26^11 + 26^12**
2. Consider the Vigenere cipher over the lowercase English alphabet, where the key has length 8. For which of the following message spaces will this scheme be perfectly secret? (Check all that apply.)
    a. **The set of all 8-character strings of lowercase English letters.**
    b. **The set of all 7-character strings of lowercase English letters.**
3. What is the result of encrypting the ASCII plaintext "cool!" using the variant Vigenere cipher (where encryption is done using byte-wise XOR) and key 0x01 3F?
    a. **0x62 50 6E 53 20**
4. Say we have a scheme with a claimed proof of security with respect to some definition, based on some assumption. The scheme was successfully attacked when used in the real world. What are possible reasons for this? (Check all that apply.)
    a. **The proof might be incorrect.**
    b. **The assumption may be false.**
    c. **The definition of security may not correctly capture the real-world threat model.**
5. In the definition of perfect secrecy, what threat model is assumed?
    a. **The attacker can eavesdrop on a single ciphertext.**
6. Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period).
    a. **Pr[C=bb] = [1/26 + 1/(26^2)] x 0.5 x 0.4 + [0 + 1/(26^2)] x 0.5 x 0.6 = 0.0084**
7. Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.4 and Pr[M='ab'] = 0.6. What is Pr[M='aa' | C='bb']? Express your answer to 4 decimal places with a leading 0, i.e., if your answer was 1/2 then you would enter 0.5000 (without a trailing period). Note: carry out the calculation exactly (i.e., do not use the truncated result that you entered as your answer in the previous question) before truncating your answer to 4 decimal places.
    a. **0.9473**

8. Which of the following are true for obtaining perfect secrecy using the one-time pad, assuming the message space contains messages all of some fixed length? (Check all that apply.)
    a. **The key must be as least as long as the messages in the message space.**
    b. **The key should be shared between the two communicating parties, and kept secret from any potential attacker.**
    c. **The key should be chosen uniformly.**
9. Consider the one-time pad over the message space of 5-bit strings, where Pr[M=00100] = 0.1 and Pr[M=11011] = 0.9. What is Pr[C=00000]? Express your answer to 5 decimal places with a leading 0. I.e., if your answer was 1/2, then you would enter 0.50000 (without a trailing period).
    a. **0.03125**
10. Which of the following are true about the Vigenere cipher? (Check all that apply.)
    a. **The Vigenere cipher is perfectly secret if the length of the key is equal to the length of the messages in the message space.**
11. Two ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0xB7 and the 10th byte of the second ciphertext is observed to be 0xE7. Let m1 (resp., m2) denote the 10th ASCII character in the first (resp., second) message. What is the most you can conclude about m1 and m2?
    a. **One of m1 or m2 is the space character, and the other is the character 'p'.**
12. Three ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be 0x66, the 10th byte of the second ciphertext is observed to be 0x32, and the 10th byte of the third ciphertext is observed to be 0x23. Let m1 (resp., m2, m3) denote the 10th ASCII character in the first (resp., second, third) message. What is the most you can conclude about m1, m2, and m3?
    a. **m1 is the space character, m2 is the character 't', and m3 is the character 'e'.**
13. Which of the following is true about computational secrecy? (Select all that apply.)
    a. **Computational secrecy currently relies on unproven assumptions.**
    b. **Computational secrecy only ensures secrecy against attackers running in some bounded amount of time.**

c. **Computational secrecy allows an attacker to learn information about the message with small probability.**

14. Let G be a function mapping n-bit inputs to 2n-bit outputs. Which of the following is true of the pseudo one-time pad encryption scheme based on G? (Check all that apply.)

    a. **The scheme is computationally secret if G is a pseudorandom generator.**

15. Which of the following attackers can be used to demonstrate that the shift cipher for 3-character messages does not satisfy perfect indistinguishability?

    a. **Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 1 if the three characters of C are all different.**

16. Which of the following is a negligible function? (Check all that apply.)

    a. **f(n) = 1/2^n**

17. Define the following function G taking n-bit inputs and producing (n+1)-bit outputs: $G(x)=x\|0$, where ‖ denotes concatenation. Which of the following attackers shows that this G is not a pseudorandom function?

    a. **On input an (n+1)-bit string y, output 0 if the last bit of y is 0.**

18. Say G is a pseudorandom generator taking n-bit inputs and producing 2n-bit outputs. Which of the following are necessarily true? (Check all that apply. The symbol '|' is used here for string concatenation.)

    a. **G(r) is computationally indistinguishable from a uniform, 2n-bit string if r is a uniform n-bit string.**

19. Which of the following is a setting in which a pseudorandom generator could be applied?

    a. **You have a way to generate random bits at the rate of 100 bits/second, but you need 1,000,000 random bits to run a statistical simulation.**

20. Consider a pseudo one-time pad encryption scheme Π constructed using some function G. Which of the following did our proof of security for the pseudo one-time pad show?

    a. **If G is a pseudorandom generator, then Π is computationally secret.**

21. True or false: any private-key encryption scheme that is CPA-secure must also be computationally indistinguishable.

    a. **True**

22. True or false: any private-key encryption scheme that is CCA-secure must also be perfectly secret.

    a. **False**

23. True or false: any private-key encryption scheme that is CCA-secure must also be CPA-secure.

    a. **True**

24. Let F be a block cipher with 128-bit block length. Consider the following encryption scheme for 256-bit messages: to encrypt message $M=m1\|m2$using key k (where $|m1|=|m2|=128$), choose random 128-bit r and compute the ciphertext $r\|Fk(r)\oplus m1\|Fk(m1)\oplus m2$. Which of the following strategies would lead to a valid chosen-plaintext attack?
    a. **Let m1 and m2 be arbitrary but distinct. Using the encryption oracle, obtain an encryption r‖ c1‖ c2 of m1‖ m2. Output messages M0=m1‖ m2 and M1=m2‖ m1. Output 0 if the third block of the challenge ciphertext is c2.**
25. Let F be a pseudorandom function with 128-bit key and 256-bit block length. Which are the following functions G are pseudorandom generators? (Select all that apply.)
    a. **G(x)=Fx(0…0)‖ Fx(1…1), where x is a 128-bit input.**
    b. **G(x)=Fx(0…0), where x is a 128-bit input.**
26. Define the keyed function F as follows: $Fk(x)=k\oplus x$. Which of the following distinguishers demonstrates that F is not a pseudorandom function?
    a. **Given access to an oracle g, query y0=g(0…0) and y1=g(1…1). Then output 1 if and only if y0⊕y1=1…1.**
27. Let F be a block cipher with n-bit block length. Consider the following encryption scheme: to encrypt a message viewed as a sequence of n-bit blocks $m1,m2,\ldots,mt$ using a key k, choose a random n-bit value r and then output the ciphertext $r,Fk(r+1+m1),Fk(r+2+m2),\ldots,Fk(r+t+mt)$, where addition is done modulo $2n$. Which of the following attackers demonstrates that this scheme is not computationally indistinguishable:
    a. **Let m be an arbitrary n-bit block, and output M0=m,m and M1=m,m−1. Given challenge ciphertext r,c1,c2, output 1 if and only if c1=c2.**
28. Say we use CBC-mode encryption based on a block cipher with 256-bit key length and 128-bit block length to encrypt a 512-bit message. How long is the resulting ciphertext?
    a. **640 bits**
29. Assume an honest user wants to send an 8-bit integer to their bank indicating how much money should be transferred to the bank account of an attacker. The user uses CTR-mode encryption based on a block cipher F with 8-bit block length. (Yes, this is a made-up example.) The attacker knows that the amount of money the user wants to transfer is exactly $16, and has compromised a router between the user and the back. The attacker receives the ciphertext 10111100 01100001 (in binary) from the user. What ciphertext should the attacker forward to the bank to initiate a transfer of exactly $32? (Recall that CTR-mode

decryption of a ciphertext $c0,c1$ using key k is done by outputting $c1 \oplus Fk(c0+1)$.)

a. 01100001 10111100

30. Assume CTR-mode encryption with PKCS #5 padding and a block cipher with 8-byte block length. Say a 4-byte message is encrypted, resulting in ciphertext 0x00 01 02 03 04 05 06 07 00 01 02 03 04 05 06 07. Which of the following ciphertexts will NOT yield an error upon decryption?

a. 0x00 01 02 03 04 05 06 07 00 01 02 04 04 05 06 07

31. True or false: CBC-mode encryption with PKCS #5 padding provides message integrity, as long as the receiver makes sure to verify the padding upon decryption.

a. False

32. Let F be a block cipher with n-bit block length. Consider the message authentication code for $2n$-bit messages defined by $\mathrm{Mac}k(m1,m2)=Fk(m1 \oplus m2)$. Which of the following gives a valid attack on this scheme?

33. Let F be a block cipher with n-bit block length. Consider the message authentication code for $2n$-bit messages defined by $\mathrm{Mac}k(m1,m2)=Fk(m1) \oplus Fk(m2)$. Which of the following gives a valid attack on this scheme?

34. Assume a sender and receiver use basic CBC-MAC but authenticate/accept messages of different lengths. Which of the following is a valid attack?

35. Assume we want to use a hash function with output length as small as possible, subject to being collision resistant against a birthday attack running in time 2192. Which hash function would be the best choice?

36. Let H,H' be collision-resistant hash functions. Which of the following functions H'' is NOT necessarily collision-resistant?

37. Assume a sender and receiver use the encrypt-and-authenticate approach for variable-length messages, using CTR-mode encryption and a variant of CBC-MAC secure for authenticating variable-length data (and independent keys for each). Which of the following statements is true?

38. Let F be a block cipher with block length n. Consider the following encryption scheme for n-bit messages: to encrypt message m using key k, choose a random $c0 \in \{0,1\}n$ and output the ciphertext $c0,c1,Fk(Fk(c0) \oplus c1)$, where $c1=Fk(c0) \oplus m$. Which of the following statements is true?

39. Which of the following is the most appropriate primitive for achieving message integrity between two users sharing a key?

40. Which of the following is an example of a message authentication code used widely in practice?

41. Consider the following algorithm for factoring an integer *N* provided as input (in binary): For *i*=2 to ⌈*N*−−√⌉, if *i* divides *N*, then output (*i*,*N*/*i*). Which of the following statements is true?
42. Which of the following is NOT a group?
43. Which of the following is the multiplicative inverse of 10 modulo 15?
44. What is [580mod79]? (Note that 79 is prime. Don't use a calculator/computer!)
45. How many elements are in the group Z∗403? (Note that 403=13·31.)
46. Which of the following gives the 3rd root of 92 modulo 187? (Note that 187=11·17.)
47. Which of the following problems is hard if the RSA assumption holds? In all the below, *N* is a product of distinct, large primes *p* and *q*, and *e* is relatively prime to *ϕ*(*N*).
48. Which of the following is a generator of Z∗13?
49. Z∗23 is a cyclic group with generator 5. In this group, what is DH5(2,20)?
50. Let *G* be a cyclic group of order *q* and with generator *g*. Based only on the assumption that the discrete-logarithm problem is hard for this group, which of the following problems is hard?
51. Which of the following is a drawback of the private-key setting that is NOT addressed by the public-key setting?
    a. **The communicating parties need the ability to generate random bits.**
52. Which of the following BEST describes the security offered by the Diffie-Hellman key-exchange protocol (assuming the DDH problem is hard)?
    a. **An attacker eavesdropping on an execution of the protocol cannot distinguish the key shared by the parties from a uniform key.**
53. Assume the Diffie-Hellman protocol is run by two parties in the subgroup of Z∗23 generated by 2. (This subgroup has order 11.) If the first party chooses private exponent 3 and the second chooses private exponent 10, which of the following characterizes the execution of the protocol in this case?
    a. **The first party sends 8, the second party sends 12, and they share the key 3.**
54. In which of the following scenarios is public-key encryption a better choice than private-key encryption?
    a. **A user wants to send his credit-card number to a merchant on the web.**
55. Which of the following would NOT be a secure way for a receiver to distribute her key for a public-key encryption scheme? (Assume a passive, eavesdropping attacker here.)
    a. **Post the private key on one's webpage.**

56. Which of the following is true in the public-key setting, but NOT true in the private-key setting?

    a. **Allowing the attacker to have access to an encryption oracle makes no difference when defining security.**

57. Assume for the purposes of this question a public-key encryption scheme for which the time to encrypt a 128-bit message is 100 times slower than the time to compute one AES evaluation. Which of the following is true if we want to encrypt a 100MB message *M*?

    a. **If hybrid encryption is used, then public-key encryption of M will take roughly the same time as private-key encryption of M.**

58. Assume El Gamal encryption, where the group being used is Z∗47 with generator 5. (This group has order 46, which is not prime. But El Gamal encryption can be defined in any cyclic group.) Assume the public key contains h=10. Say an attacker sees a ciphertext (41, 18) that is the encryption of some unknown message m. Which of the following is an encryption of [5*m*mod47]?

    a. **(41, 43)**

59. Assume "plain RSA" encryption is used with public key (N=33,e=3). What is the encryption of the message m=2?

    a. **8**

60. Which of the following is true about "plain RSA" encryption (assuming the RSA problem is hard)?

    a. **If the message m is uniform in ℤ∗ N, then m cannot be recovered in its entirety from the ciphertext in polynomial time.**

61. The Federal Government wants to be able to issue advisories to the general public while ensuring that no one will be able to tamper with their messages or spoof a fake advisory. Which of the following is the best cryptographic approach to address this problem?

62. The president and vice president of a company want to communicate while ensuring integrity of their communication. Which of the following is the best cryptographic approach to address this problem?

63. Assume for the purposes of this question a digital signature scheme for which the time to sign a 256-bit message is 100 times slower than the time to evaluate SHA-256 on a 512-bit input. Which of the following is true if we want to sign a 500MB message *M*?

64. Assume the "plain" RSA signature scheme, with public key (N=55,e=3). Which of the following verifies correctly as the signature on the message m=17?

65. Assume the "plain" RSA signature scheme with public key $(N,e=3)$. For which of the following messages is it always possible to forge a signature without seeing any prior signatures or factoring N? (Assume $N>1000$, and N relatively prime to each of the messages that follow.)

66. Assume the "plain" RSA signature scheme with public key (N,e). Say we want to forge a signature on $m=289$ but can only obtain a signature on one other message. Which of the following strategies will work? (Assume $N>1000$.)

67. In this and the next question, assume the Schnorr identification protocol is run in the subgroup of $Z*23$ generated by 2. (This subgroup has order 11.) Say the prover's private key is $x=7$. What is the prover's public key?

68. (This is a continuation of the previous question.) Say the prover runs an execution of the Schnorr identification protocol with a verifier. The prover chooses $r=4$ and sends $A=16$. The verifier sends challenge 3. What response does the prover send?

69. As in the lectures, let $\mathrm{cert}A\rightarrow B$ denote a certificate issued by A for B, i.e., $\mathrm{cert}A\rightarrow B=\mathrm{Sign}skA(B,pkB)$. Assuming D knows pkC and trusts C, which of the following provides evidence to D that A's public key is pkA?

70. Consider the SSL/TLS handshake protocol as described on slide 5 of the SSL/TLS lecture. Say the encryption of *pmk* were changed from using a CCA-secure public-key encryption scheme to using a CPA-secure public-key encryption scheme. Which of the following attacks would this change potentially enable?

71. What is the most appropriate cryptographic primitive to use if a company wants to distribute authenticated software updates to its customers?

72. What is the most appropriate cryptographic primitive to use if an individual wants to ensure confidentiality of the files stored on her hard drive?

73. A user wants to design a CPA-secure public-key encryption scheme to be used for emailing large files. Of the following, which would be the best approach?

74. Consider the following "hybrid" signature scheme, which will give better efficiency when signing long messages. To sign message M using private key sk, choose a uniform key k for a message authentication code and then send $k,\mathrm{Sign}sk(k),\mathrm{Mac}k(M)$. Verification is done in the natural way. Which of the following is true regarding this scheme?

75. Let G be a group, and consider the following private-key encryption scheme with message space G: The shared key is a uniform element $k\in G$. To encrypt a message $m\in G$ using key k, output the ciphertext $k\cdot m$. To decrypt a ciphertext $c\in G$ using key k, output the message $k-1\cdot c$. Which of the following is true about this scheme?

76. Consider hybrid encryption using plain RSA and AES-128 in CTR mode, with public key N,e. Say a 128-bit message m is encrypted, yielding ciphertext $c,c0,c1$, with $c \in Z*N$ and $c0,c1 \in \{0,1\}128$. Which of the following would be an encryption of $\overline{m}$, the bitwise complement of m?

77. Say El Gamal encryption is used in the subgroup of $Z*47$ generated by 4. The public key is 21 and the private key is 4. The ciphertext (34,42) is an encryption of some message m. Which of the following is an encryption of $[4m\text{mod}47]$?

78. Consider the plain RSA encryption scheme with public key $N=55,e=3$. Say the encryption of some unknown message m is 6. What is the encryption of $[2m\text{mod}N]$?

79. Say you have "oracle access" to a piece of code that, given a message m, appends an unknown 8-byte password p, applies PKCS #7 padding, and then encrypts the result using AES-128 in ECB mode with an unknown key. Which of the following attacks can be used to confirm that the first byte of p is 'Z'?