

ENTS 689i
Exam 1, Fall 2008
Thursday, October 2

Multiple Choice (2 points each)

Circle the letter of the response that best answers the question.

1. Which of the following is not a fundamental security goal?
 - a. Confidentiality
 - b. Integrity
 - c. Assurance
 - d. Availability
2. Disclosure is a threat against which security goal?
 - a. Confidentiality
 - b. Integrity
 - c. Assurance
 - d. Availability
3. Which of the following security properties does an S-Box provide?
 - a. Diffusion
 - b. Integrity
 - c. Malleability
 - d. Confusion
4. Which of the following security properties does a P-Box provide?
 - a. Diffusion
 - b. Integrity
 - c. Malleability
 - d. Confusion
5. Which of the following ciphers suffers from malleability attacks?
 - a. DES
 - b. 3DES
 - c. RC4
 - d. AES
6. Which of the following encryption modes suffer from malleability attacks?
 - a. Electronic Code Book (ECB)
 - b. Cipher Block Chaining (CBC)
 - c. Offset Code Book (OCB)
 - d. Counter CBC-MAC (CCM)
7. Which of the following hash functions is still considered secure against collision attacks?
 - a. SHA-1
 - b. SHA-256
 - c. MD-4
 - d. MD-5

Name _____

- 8. In order for a cipher to be considered secure, decryption without the key should be which of the two following complexity classes:
 - a. Linear
 - b. Polynomial
 - c. Nondeterministic Polynomial
 - d. Exponential

Short Answer (4 points each)

Answer each of the questions in 2-3 sentences.

- 9. Describe the capabilities of an off-path active adversary.

Spoofing, injection of packets; cannot see traffic but can transmit; denial of service

- 10. Describe how to perform cryptanalysis on a message encrypted with a Vigenère cipher.

Since the length-N password is repeated, you can break the ciphertext into N interleaved Caesar ciphers with arbitrary rotations, and perform frequency analysis on each

Name _____

11. What are the advantages and disadvantages of a One-Time Pad?

Advantages: perfect secrecy means passive cryptanalysis is impossible

Disadvantages: key same length as password and difficult to transport and synchronize; keys not reusable; suffers from a lack of diffusion

12. What are the advantages of using mutual key derivation over key wrapping for key distribution.

Guaranteed entropy because both sides contribute; key never transmitted over the network;

Key agreement protocols can also be used for mutual authentication.

13. Describe the meet in the middle attack against 3DES.

For plaintext P and ciphertext C, compute $Y=D(C, k_3)$ for all k_3 . Then compute $X=D(E(P, k_1), k_2)$ for all k_1 and k_2 until a value is found such that $X=Y$. Attack complexity is $O(2^{112})$ rather than $O(2^{168})$.

Name _____

14. How can ciphers susceptible to malleability attacks be protected?

For malleable ciphers, include a cryptographic hash or message integrity code.

For malleable encryption modes, use a chaining mode such as CBC.

15. Describe the difference between preimage resistance and collision resistance for a cryptographic hash function.

$H = \text{Hash}(M)$

Preimage: given H , computing M should be an exponential problem

Collision: given H, M , finding M' such that $H = \text{Hash}(M')$ should be an exponential problem

16. What is the most computationally efficient way to attack an RSA-based cryptosystem, given access to the public key and cipher text?

Factor the modulus to find $\Phi(\text{modulus})$ and use that to invert the public exponent to find the private exponent.

Name _____

17. What are the advantages of Elliptic Curve Cryptography over RSA?

ECC's security is based on the DL problem rather than factoring problem, and is therefore

more secure, which allows for smaller key sizes that's more efficient to compute.

Quantitative Problems (8 points each)

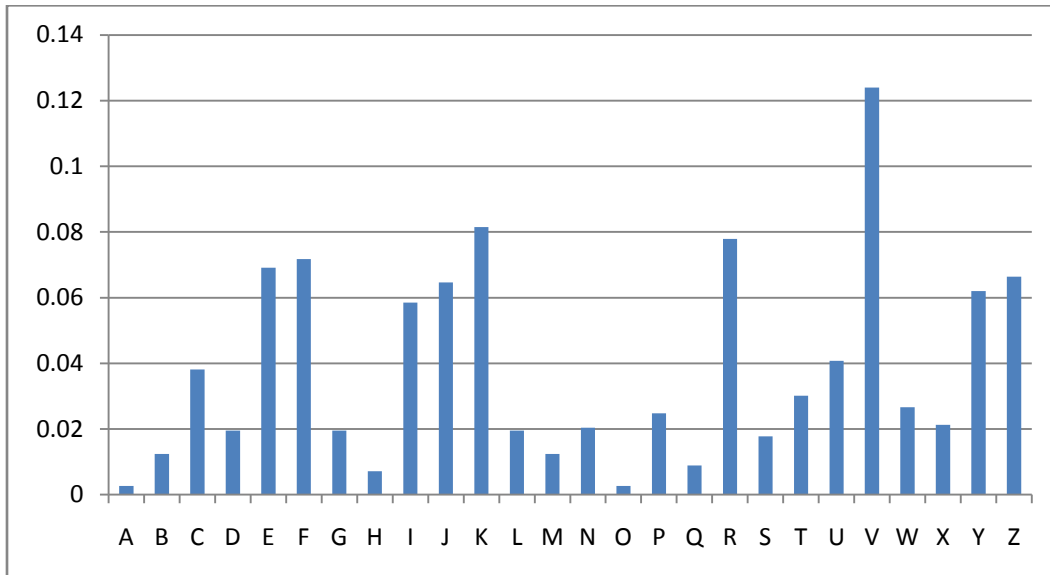
18. Decrypt the following message encrypted with the classic Caesar cipher.

K	L	G	G	H	Q
H	I	D	D	E	N

Since the classic Caesar cipher is simply a rotation by 3, for each character select the character 3 earlier in the alphabet.

Name _____

19. A long message was encrypted with a rotation cipher. Its frequency analysis reveals the following probability distribution:



Use this information to decrypt the following portion of the message:

T	F	E	W	Z	U	V	E	K	Z	R	C
C	O	N	F	I	D	E	N	T	I	A	L

Since "V" is the most used character, assign V=E and wrap the alphabet around to decode.

20. An RSA system has modulus $m=9$ and encryption exponent $e=3$. Encrypt the message $P=5$.

$$\begin{aligned}
 C &= P^e \pmod{m} \\
 &= 5^3 \pmod{9} \\
 &= 25 \times 5 \pmod{9} \\
 &= 7 \times 5 \pmod{9} \\
 &= 35 \pmod{9} \\
 &= \underline{8} \pmod{9}
 \end{aligned}$$

Name _____

21. Assume it takes 10ms to encrypt a block of data using a public-key cipher, 1ms to encrypt a block of data using a private-key cipher, and a symmetric key is 9 block long. A message is a set of data blocks, and can either be encrypted in its entirety with a public-key cipher, or a symmetric key can be encrypted using a public-key cipher, and the message can be encrypted using a symmetric-key cipher. How long does a message need to be in order for using symmetric key encryption to be computationally faster?

L = length

Time for Public Key: $10 \times L$

Time for Symmetric Key: $L + 9 \times 10$

$$10 \times L = L + 90$$

$$\underline{L = 10}$$

22. Encrypt the message {1, 0, 0, 1, 1, 0, 1, 1} using the following "regular" knapsack {5, 10, 3, 7, 12, 6, 1, 8}.

$$\{1, 0, 0, 1, 1, 0, 1, 1\} \times \{5, 10, 3, 7, 12, 6, 1, 8\} = 5 + 7 + 12 + 1 + 8 = \underline{33}$$

SOLUTIONS

Name _____

23. Quantum transmitter assigns 0 to \Rightarrow or \Leftarrow , 1 to \Uparrow or \Downarrow . The sender transmits {1, 0, 1, 1, 0, 0, 1, 1} as photon orientations $\{\Uparrow, \Rightarrow, \Downarrow, \Uparrow, \Leftarrow, \Rightarrow, \Downarrow, \Uparrow\}$. The receiver uses receive filters $\{x, +, +, +, x, +, x, +\}$. Using "1", "0", and "?", determine the received signal.

Filters for bits 1 and 3 were misaligned. Therefore the received value is {?, 0, ?, 1, 0, 0, 1, 1}.