

CS 134: MIDTERM

10. Problem 1:

What are the four main **types of attacks** on encryption algorithms? Describe each.

10. Problem 2:

What are the common **modes of operation** for a conventional cipher, such as DES or AES? Explain how each one works.

10. Problem 3:

You're at a geek party where the host plays the following game:

- He asks each guest to dip a hand in a barrel which has 400 tickets and pick one
- Each ticket has a number between 1 and 400 (inclusive)
- Each guest remembers the number on the ticket and puts the ticket back into the barrel
- Each guest is then supposed to find a partner – a person whose ticket number PLUS the guest's own ticket number EQUAL 401.

What does the number of guests at the party need to be for you to have at least 50% chance of not finding a partner?

10 (3+3+4). Problem 4:

1. Calculate $\phi(77)$ and $\phi(\phi(77))$
2. What is the order of the group Z_{35}^* ?
3. What is the order of each element in Z_7^* ?

10. Problem 5:

Alice creates a new hash function from DES. She takes message M and splits it into 64-bit blocks $M_1 \dots M_t$. She then defines a hash of M as the XOR of all blocks encrypted with DES with some known (not secret) key K . In other words $H(M) = \text{DES}(K, M_1) \text{ XOR } \text{DES}(K, M_2) \text{ XOR } \dots \text{ XOR } \text{DES}(K, M_t)$. You can assume that Alice then sends $M, H(M)$ to Bob.

Is this a good hash function? In either case, explain/justify your answer.

10 (5+5). Problem 6:

1. What is a better cipher: Affine or Caesar? Why?
2. What (if any) are the problems with the Permutation cipher? (Assume we're encrypting one alphabet letter at a time and the ciphertext is also alphabetic).

10. (4+3+3). Problem 7:

Recall El Gamal encryption (where $y = b^x \pmod p$ is the public key of the decryptor – Bob)

1. generate random r
2. ciphertext is: $c = my^r \pmod p$, $k = b^r \pmod p$

What happens if:

- a) Alice re-uses the same r in encrypting 2 different messages m_1 and m_2 ?
- b) Alice accidentally reveals r used in encrypting a message m ?
- c) Alice encrypts the same message twice (but with different r -s)

10 (5+5). Problem 8:

- (a) Bob chooses an RSA modulus $n = 13 \times 7 = 91$. He wants an easy-to-remember encryption exponent, so he wants to use either $e = 25$ (his age) or $e = 12$ (the size of his shoes). Which one(s) won't work and why?
- (b) Alice picks another RSA modulus $n = 5 \times 11 = 55$. She picks $e=3$. What is Alice's decryption exponent d ?

