CIS 5371 Cryptography

QUIZ 1 (5 minutes only) with answers

This quiz concerns the Intro to Number Theory discussion and basics of cryptography.

1. Fermat’s Little theorem states that:
   For every prime number \( p \) and number \( a \) with \( 0 \leq a < p \) we have: \( a^p = a \mod p \).
   (accept also: number \( a \) with \( 0 < a < p \) we have: \( a^{p-1} = 1 \mod p \).)

2. Let \( p, q \) be primes, \( n = pq \), and \( a \in Z^*_n \). Is it true that \( a^n-1 = a \mod n \)?
   Answer: NO.

3. For \( p = 5 \), \( q = 7 \), is it true that: \( a^{25} = a \mod 35 \)?
   Answer: YES.

4. Bob says: “An encryption scheme is secure if no adversary can find the secret key given the ciphertext”. Alice disagrees. Is she right and if so, why?
   Answer: She is right. It may be possible to decrypt the ciphertext (break the system) without the key, or at least get some useful information regarding the plaintext without decrypting.

Mike Burmester