CSE 484 In-Class Worksheet #14 – Autumn 2019

Name: _____ UWNetID: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: How do you decrypt a message encrypted with CBC mode? (See figures on back.)

Q2: Why might you want to use CTR mode instead of CBC mode?

Q2: Do CTR mode or CBC mode protect the integrity of messages? If so, why? If not, can you give a counter example?

Q3: Given these RSA parameters: p=7, q=11, e=7. Recall that the public key would be (N,e) and the private key would be (N,d). Calculators / Web Tools OK.

What is N?

What is $\phi(N)$?

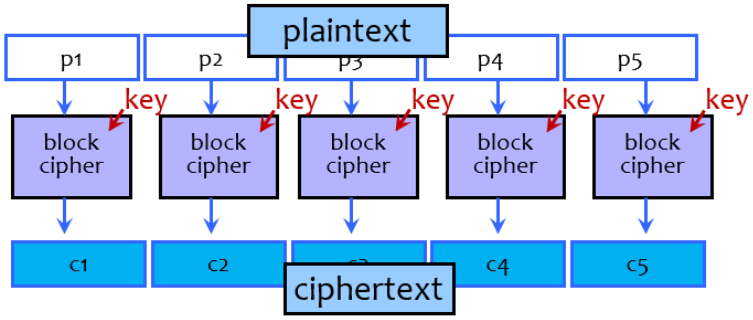
What is d?

Given these parameters, encrypt 16.

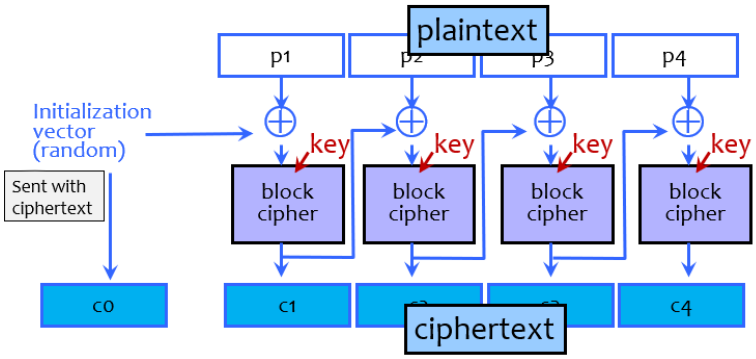
Given the parameters, decrypt 15.

What would d be if e=3? (Trick question.)

Electronic Code Book (ECB) Mode



Cipher Block Chaining (CBC) Mode: Encryption



Counter Mode (CTR): Encryption