**UBI528/UTI502 Network Security**

**Homework #4**

**Review Problems**

**R1.** Operational devices such as firewalls and intrusion detection systems are useful to counter attacks against an organization’s network. What is the basic difference between a firewall and an intrusion detection system?

**R2**. Internet entities (routers, switches, DNS servers, Web Servers, user end systems, and so an) often need to communicate securely. Give three specific example pairs of Internet entities that may want secure communication.

**R3**. The encryption technique itself is known-published, standardized, and available to everyone, even a potential intruder. Then where does the security of an encryption technique come from?

**R4**. What is the difference between known plaintext attack and chosen plaintext attack?

**R5**. Consider a 16-block cipher. How many possible input blocks does this cipher have? How many possible mappings are there? If we view each mapping as a key, then how many possible keys does this cipher have?

**Problems**

**P1.** Show that Trudy’s known-plaintext attack, in which she knows the (ciphertext, plaintext) translation pairs for seven letters, reduces the number of possible substitutions to be checked in a monoalphabetical cipher by approximately 109.

**P6**. Consider the 3-bit block cipher as:

 Suppose the plaintext is 100100100.

**a)** Initially assume that CBC is not used. What is the resulting ciphertext?

**b)** Suppose Trudy sniffs the ciphertext. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn’t koow the specific cipher), what can she surmise?

**c)** Now suppose that CBC is used with IV = 111. What is the resulting ciphertext.

**P8**. Consider RSA with *p*=7 and *q*=13.

1. What are *n* and *z*?
2. Let *e* be 17. Why is this an accepable choice for *e*?
3. Find *d* such that *de*=1 (mod *z*).
4. Encrypt the message *m*=9 using the key (*n*, *e*). Let c denote the corresponding ciphertext. Show all work.