**Handout - Worksheet 4.5 & 4.6 - Applications of Congruences and Cryptography**

**Hashing Functions**: A hashing function $h$ assigns memory location $h(k)$ to the record that has $k$ as its key. One of the most common hashing functions is the function

$$h(k) = k \mod m$$

where $m$ is the number of available memory locations.

**Pseudorandom Numbers**: The most commonly used procedure for generating pseudorandom numbers is the linear congruential method.

We choose four integers: the **modulus** $m$, **multiplier** $a$, **increment** $c$, and **seed** $x_0$, with $2 \leq a < m$, $0 \leq c < m$, and $0 \leq x_0 < m$. We generate a sequence of pseudorandom numbers $x_n$, with $0 \leq x_n < m$ for all $n$, by successively using the recursively defined function $x_{n+1} = (ax_n + c) \mod m$.

Many computer experiments require the generation of pseudorandom numbers between 0 and 1. To generate such numbers, we divide numbers generated with a linear congruential generator by the modulus: that is, we use the numbers $x_n/m$.

A **cryptosystem** is a five-tuple $(P, C, K, E, D)$, where $P$ is the set of plaintext strings, $C$is the set of ciphertext strings, $K$ is the keyspace (the set of all possible keys), $E$ is the set of encryption functions, and $D$ is the set of decryption functions.We denote by $E_k$ the encryption function in $E$ corresponding to the key $k$ and $D_k$ the decryption function in $D$ that decrypts ciphertext that was encrypted using $E_k$, that is $D_k(E_k(p)) = p$, for all plaintext strings $p$.

1. Which memory locations are assigned by the hashing function $h(k) = k \mod 101$ to the records of insurance company customers with these Social Security numbers?
   (a) 104578690
   (b) 432222187
2. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1) \mod 7$ with seed $x_0 = 3$?
3. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the encryption function $f(p) = (p + 4) \mod 26$, and then translating the numbers back into letters.
4. Decrypt this message encrypted using the shift cipher $f(p) = (p + 10) \mod 26$.

$$CEBBOXNOBXYG$$