Indian Institute of Technology, Delhi

Major

COL 759 Cryptography and Computer Security

MM 100

1. (7 marks) Determine whether or not the congruence $x^2 + 6x - 50 \equiv 0 \pmod{79}$ has a solution.

2. (23 marks) In a guest house of 50 rooms, it is planned to have an electronic card accessibility for the visitors. There is a receptionist who issues a new electronic card to the guest on his/her arrival from a machine, kept in a secure location. The room can only be opened after showing the electronic card to electronic card readers which is installed on the doors of the rooms. The card reader has a microcontroller which has computation power and little storage (64 bytes). Once the room is opened by a new guest, all the previously issued cards of that room should not work. There is no communication (wired/unwired) between the card issuing machine and the card reader. Assume that attacker/intruder can have complete access to the card reader but cannot access the card issuing machine.
   Design a scheme for this accessibility system and explain clearly the protocols followed by the card reader as well as key issuing machine in the system.

3. (15 marks) Assume there is only one honest prover (A) and one honest verifier (B). A trusted third party (C) generates a large composite number n, which is a product of two primes p and q. In addition, C generates a public RSA exponent e and a private RSA exponent d. C publishes n and e but keeps p, q and d secret.
   Suppose A's public identity is I. C then gives the prover the value $F = I^{-d} \bmod n$, which is served as his/her secret.
   The identification protocol then consists of 4 steps and can be described as follows:

   (i) The prover chooses a random number $r \in Z_n^*$ and computes $T = r^e \bmod n$. Prover A then sends T to the verifier B and keeps r secret.
   (ii) B chooses a random number c in $\{0, 1, \ldots, e-1\}$ and sends c to A.
   (iii) A computes $t = r \cdot F^c \bmod n$ and sends t to B.
   (iv) B accepts the identification if and only if $T = I^c \cdot t^e \bmod n$.

   (a) Show that $T = I^c \cdot t^e \bmod n$.
   (b) Suppose B knows a factor modulus (p and q). Explain how B can learn A's secret (i.e. F) from this protocol.

(c) Suppose a malicious prover knows c ahead of time (i.e., before the start of the protocol). Explain how the malicious prover can impersonate the prover A without needing to know F, d, p or q.

4. (35 marks) Consider a situation that you (as cryptanalyst) know at least $2n$ bits of the LFSR based ciphertext sequence but the bits known are not necessarily consecutive.
   Example: Assume that the system uses a 5-stage linear feedback shift register and that you, as cryptanalyst, know 12 bits. Assume they are spaced as follows:

   1?101?00?1??1?11???11

   The question marks merely denote positions of the sequence for which you do not know the entry.
   How can you analyze the ciphertext? Find all the missing bits of the sequence in the example.

5. (20 marks) An affine block cipher is one where the key specifies a non-singular s by s matrix **A** and an s-tuple **t** to define the affine transformation **c** = **Am** + **t** where , **m** is a block of plaintext (size s) and **c** is the corresponding ciphertext. **c**, **A** and **m** all are over GF(2). Show that the number of affine transformations are

   $$2^s (2^s - 1) (2^s - 2) (2^s - 2^2) \ldots (2^s - 2^{s-1}).$$