Indian Institute of Technology, Kharagpur
Department of Computer Science and Engineering
End Spring Semester 2011

Subject – Cryptography and Network Security, Subject No. – CS60041
Full Marks – 100, Date – 25th November, 2011, AN, Time – 3 hrs.

Answer any 5 questions

1(a). In the RSA algorithm show that “e” must be odd.

(b) Suppose Bob has an RSA cryptosystem with modulus n and encryption exponent b_1 and Charlie has an RSA cryptosystem with the same modulus n and encryption exponent b_2. Suppose that $\gcd(b_1, b_2) = 1$. Now, consider the situation that arises if Alice encrypts the same plaintext x using RSA to send to both Bob and Charlie. Let y_1 and y_2 are sent to Bob and Charlie. Suppose Oscar intercepts the messages sent to Bob and Charlie and performs the following computations

```
{
  $c_1 = b_1^{-1} \bmod b_2$
  $c_2 = (c_1 b_1 - 1)/b_2$
  $x_1 = y_1^{c1} (y_2^{c2})^{-1} \bmod n$
  return ($x_1$)
}
```

Prove that Oscar can decrypt the message Alice sent i.e. the value x_1, computed is in fact Alice’s plain text x.

(b) What are conventional approaches to attack RSA mathematically?
“Security of RSA depends on the performance of the algorithm for computing prime factors” – Justify.

[2+10+8=20]

2(a) What is the primitive root of a number? Find all the primitive roots of 12.

(b) Brifly explain Diffie-Hellman key exchange.

(b) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root p = 3.

(i) if user Alice has public key $Y_A = 7$, what is Alice’s private key X_A?

(ii) If user Bob has public key $Y_B = 9$, what is the shared secret key K?

[6+6+8+20]

3(a) Define Euler-Totient function φ(n). Suppose an eavesdropper Eve knows N = pq and also knows φ(N) = (p-1)(q-1), Show that Eve can then find p and q.

(b) State RSA algorithm by clearly explaining the key generation.

(c) Suppose Tom wishes to send a text message M to Jerry using the RSA algorithm. Jerry’s public key is the pair (n, e) = (253, 13). Note that 253 = (23)(11) and $(17)(13) \equiv 1 (\bmod 220)$. Tom uses an alphabet set of only 10 letters and encodes them as

A = 0, C = 1, D = 2, G = 3, I = 4, N = 5, O = 6, R = 7, T = 8, U = 9.

Tom transmits the message in blocks. Each block corresponds to two letters which are encoded into their numerical equivalents, e.g. CU becomes [19] and then it is enciphered by using RSA.

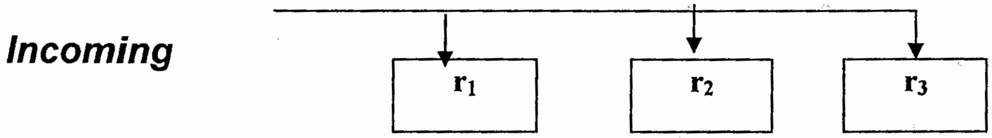
(i) if Tom wants to send the text "GO", what cipher will be received by Jerry?

(ii) if Jerry receives the cipher text [11], what was the message transmitted by Tom?

[5+5+(5+5)=20]

4(a) State Chinese Remainder Theorem. Is the requirement that the moduli be pair-wise relatively prime in CRT necessary? What happens if we remove the restriction?

(b) Imagine that you have three counters commonly counting a train of pulses as depicted in the figure below



Counter i is started at zero and counts up to $c_i - 1$ and then resets to zero at the next count. The count of counter i is displayed as r_i.
Let $(c_1, c_2, c_3) = (3, 5, 7)$. If at the counting pulses, the counters' counts are $(r_1, r_2, r_3) = (1, 0, 6)$, what is the minimum number of pulses that were counted?

(c) Given an enciphering scheme e = 3, show how a plain text message M can be recovered if it is enciphered and sent to –different entities having pairwise relatively prime moduli N_1, N_2, N_3.

[5+10+5=20]

5(a) What is an Elliptic curve?

(b) What is the zero point of an elliptic curve?

(c) One elliptic curve encryption/decryption is to be performed over Z_{11}. The cryptosystem parameters are $E_{11}(1,6)$ and the base point G = (2,7). Part B's secret key is $n_B = 7$.

(i) Find B's public key P_B.

(ii) If Party A wishes to encrypt the message $P_m = (10,9)$ and chooses the random value k = 3, determine the ciphertext C_m.

(iii) Show the calculation by which B recovers P_m from C_m

[4+4+12=20]

6(a) What characteristics are needed in a secure hash function?

(b) Assume in an authentication scheme, the hash function used is H and the encryption /decryption function is E/D. Show how the function will be used to provide authentication as well as confidentiality.

(c) Let b be a byte in bit form and let b' be B + 11111111 (the complement of b). for a fixed given key, if AES encrypts b to g, does AES encrypt b' to g'. Justify your answer.

(d) Describe the stream cipher "Grain" with a proper diagram.

[5+5+5+5=20]