Indian Institute of Technology, Delhi

Major

COL 759 Cryptography and Computer Security

Time: 2 Hour and 40 Minutes Max. Marks 100

Don't ask doubts. Please use your judgement.

1. (5 marks) Consider prime p of the form $p = 3 \cdot 2^n + 1$, where n is a natural number. Prove that 2 is not a primitive root modulo p except for $n = 2$.

2. (5 marks) A message of size 1000 characters using a four letter ('a', 'b', 'c', 'd'), language is encrypted with Vigenère Cipher. The probabilities of the letters 'a', 'b', 'c' in the language are 0.5, 0.15 and 0.3 respectively. This encrypted message is required to be analyzed using index of coincidence. How many largest coincidences are likely to see in this message?

3. (5 marks) Prove that for odd n, $n|2^{n!} - 1$.

4. (5 marks) Suppose A and B use RSA cryptosystem for secure communication. They have generated public keys (n, e) and (n', e') using a prime p (i.e., $n = pq$ and $n' = pq'$). Is it possible for the cryptanalyst to find their private keys? Explain.

5. (5 marks) Prove that 31803221 is not a prime number.

   Given $2^{31803212} \equiv 27696377 \pmod{31803221}$.

6. (5 marks) Find the number of solutions in ordered pairs of positive integers (x, y) of the equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{84}$.

7. (5 marks) In the finite field $F_2[x]$ modulo $x^8 + x^4 + x^3 + x + 1$, find the inverse of element x of the field.

8. (5 marks) Let $E(F_{2^4})$: $y^2 + y = x^3$. Show that every $P \in E(F_{2^4})$ is a point of order 3.

9. (5 marks) Find all $c \in Z_3$ such that $Z_3[x]/(x^3 + cx^2 + 1)$ is a field.

10. (6 marks) How many zeros should be padded to a message of length 4000 bits to find hash value using SHA-3 (Keccak) with security strength 512 bits?

11. (7 marks) In DES S-box transforms 6 bits of input to an output of 4 bits i.e., S: $\{0,1\}^6 \rightarrow \{0,1\}^4$. It seems that some data might have lost, and the function is not invertible. But still DES decryption gives the correct output. Explain how?

12. (7 marks) In AES (Rijndael) Shift Rows and Byte Substitution layers can be applies in any order with the same result. Explain how it is possible.

13. (7 marks) Suppose the two users agreed to use ElGamal Signature Scheme in digital signature. If the signer has used the same random number k for transmitting two different messages, then is it possible for the interceptor to find the secret key d? Explain.

14. (8 marks) Let α be a primitive root modulo a large prime p. A hash function h: $Z \rightarrow Z_p^*$ defined as $h(m) = \alpha^m \bmod p \ \ \forall m \in Z$. Is this hash function

    (a) pre-image resistant?

    (b) collision resistant?

    Justify your answers.

15. (10 marks; 2 marks each)

    (a) The security of many recently proposed cryptosystems is based on the difficulty of solving large systems of quadratic multivariate polynomial equations. This problem is NP-hard over any field. Name the polynomial time algorithm to solve such a system of equations when the number of equations m is the same as the number of unknowns n and $n \geq 15$.

    (b) AES uses operations in the two fields GF(2^8) and GF(2). BES (a block cipher), presented in the class, uses only simple algebraic operations in only one field. What is the order of that field?

    (c) There is a variety of cryptographic mechanisms which can be used to safeguard the confidentiality and integrity of stored and transmitted information. In case of embedded systems, because of its resource constraint nature only a special class of cryptographic algorithms can be used. What type of algorithms are suitable for these embedded systems?

    (d) How fingerprint biometric can be used as an alternate to maintain the privacy of cryptographic key?

    (e) Why is it considered that the low degree LFSR based Random Number Generators (RNG) are easily predictable?

16. (10 marks) A 4-stage LFSR with feedback polynomial C(x) = $x^4 + x + 1$ is used for transmission of secret messages by A. To make the encryption process more secure, A uses every second bit of the sequence generated by the LFSR instead of every bit generated by the LFSR. i.e.,

    $$c_i = m_i \oplus s_{2i} \ \text{ for all } i = 1, 2, \ldots, n \text{ (length of the message).}$$

    Where m_i and c_i are the i^{th} bit of the message and ciphertext respectively. s_{2i} is $(2i)^{\text{th}}$ bit of the key stream generated by the LFSR.

    Suppose you as cryptanalyst intercepted the first 7 bits of ciphertext sequence 0 1 1 1 1 1 0 and you know that the first 4 bits of the message are 1 1 1 1. Find the entire message.