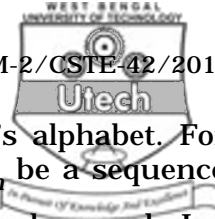


Invigilator's Signature :

[Turn over



3. a) Describe Chen's authenticated encryption scheme.
b) Describe briefly the Alert protocol and Record Protocol in SSL. 7 + 7
4. a) It is tempting to try to develop a variation on Diffie-Hellman that could be used as a digital signature. Here is one that is simpler than DSA and that does not require a secret random number in addition to the private key.
- Public elements : p (prime number),
 g (generator of Z_p)
- Private key : x , $1 < x < p - 1$.
- Public key : $y = g^x \text{ mod } p$.
- To sign a message M , compute $h = H (M)$, where $H()$ is a cryptographically strong hash function. Assume that $\gcd (h, p - 1) = 1$. (If not, append the hash to the message and recalculate the hash. Continue this process until a hash is generated that is relatively prime to $p - 1$). Then calculate Z to satisfy $Z \times h = x \text{ mod } p - 1$. The signature of the message is $s = g^Z$. To verify a signature a user verifies that $s^h = y$. (Should hold for good signatures because $s^h = (g^Z)^h = g^x = y$). Show that the verification process produces an equality if the signature is valid.
- b) Describe a smart-card authentication protocol based on hash function. 7 + 7
5. a) Describe a Needham and Schroeder's 'challenge response' protocol.
- b) Describe Zero-knowledge authentication protocol based on DLP. 7 + 7



6. a) Let s be the size of a natural language's alphabet. For English $s = 26$. Let $k = k_1, k_2, \dots, k_n$ be a sequence of characters in the alphabet called the keyword. Let $e()$ be an arbitrary permutation of the alphabet's characters (not necessarily a shift). The single mixed-alphabet Vigenere cipher with secret key $(k, e())$ is defined as follows: $c_i = e(m_i) + k_i \bmod s$, where c_i is the i th character of the ciphertext, encrypting the i th character m_i of the plaintext. As in the regular Vigenere cipher, $k_{i+n} = k_i$ if $i > n$: The characters of the key-word are reused cyclically. The corresponding decryption algorithm is $m_i = e^{-1}(c_i - k_i \bmod s)$. Analyze the security of the above system.
- b) Describe Kerberos V5 authentication protocol. 7 + 7
7. a) Define Bilinear pairings. Design a multi-signature scheme based on bi-linear pairings.
- b) Describe PGP file format and Radix-64 conversion technique. 7 + 7
8. Write short notes on the following :
- a) SET
- b) SMIME
- c) IP security. 5 + 5 + 4
