IIT Jodhpur

CSL-7480 Cryptography May 2021

End-term exam Instructor: Somitra Sanadhya

Time: 2 hours Max. Marks: 40

---

1. Let $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{C} = \{1, 2, 3, 4\}$ and Pr[P=$a$] = 1/4, Pr[P=$b$] = 3/10, Pr[P=$c$] = 3/20 and Pr[P=$d$] = 3/10. Further, let $\mathcal{K} = \{k_1, k_2, k_3\}$ and Pr[K=$k_1$] = 1/4, Pr[K=$k_2$] = 1/2 and Pr[K=$k_3$] = 1/4. The encryption function is given by the table below.

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $k_1$ | 3 | 4 | 2 | 1 |
| $k_2$ | 3 | 1 | 4 | 2 |
| $k_3$ | 4 | 3 | 1 | 2 |

   Compute the following from the given data:

   (a) Pr[C=1 | P=$c$]

   (b) Pr[C=4]

   (c) Pr[P=$d$ | C=2]

   (d) Pr[P=$c$ | C=4]

   Is the given cipher perfectly secure ? (4 marks)

2. A "block cipher distinguisher" is an algorithm which can predict with high probability whether a system is a random permutation or a block cipher, by asking few queries to the system. Propose a distinguisher for 2-round DES. What is the probability of success of your distinguisher ? [4 Marks]

3. AES uses a SPN structure where SBox, ShiftRow, MixColumn and AddRoundKey operations are applied one by one a total of $r$ times (where $r$=10 for AES-128 etc). Your friend decides to make the successor of AES, let us call it BFT, where he suggests using $r$ rounds of SBox operations, followed by $r$ rounds of ShiftRow and MixColumn operations and finally $r$ rounds of AddRoundKey. How secure is this new design ? Does it achieve same or higher or lower level of security than AES ? Justify your answer. [4 Marks]

4. (a) State (no need to prove) the key complementation property of DES.

   (b) How can it be used in key search ? (Explain the cost of the key search with the use of this property.)

   [4 Marks]

5. Mr Banerji, Mr Chatterji and Mr Das are using the same public exponent 3 but different RSA moduli $n_B$, $n_C$ and $n_D$ respectively. Mr Adhikari sent the same message $m$ to all three of them, by appropriately encrypting the message with textbook RSA encryption algorithm. Show that an eavesdropping adversary can decipher $m$ from the given information. [4 Marks]

6. A block cipher is being used in a certain mode of operation. The $i$th encrypted block gets corrupted on the way to the receiver. What will be the effect of this error on the receiving side (when she tries to decrypt), if the mode of operation is: (a) ECB (b) CBC. [4 Marks]

7. Explain what is meant by the following two properties for a hash function. Give one use-case for each of these properties (i.e. a situation for each of these cases where the property is useful in real life).

   (a) Preimage resistance

   (b) Collision resistance.

   [4 Marks]

8. An elliptic curve $E$ is described by the modular equation $y^2 \equiv x^3 + x + 6 \pmod{11}$. A point $P$ on the curve is (2,7). Find the point $2P$ on the curve. [4 Marks]

9. Let $SIG$ be a secure public key signature (such as RSA) algorithm which works on $\ell$-bit strings. Let $M_k$ be the set of all $k\ell$-bit strings ($k > 1$).

   (a) Let $m \in M_k$ be $m = m_1||m_2||\ldots||m_k$ with each $m_i \in \{0,1\}^\ell$. We define a signature algorithm $SIG_1$ which works on the string $m$ as:

   $$SIG_1(m) = SIG(m_1)||SIG(m_2)||\ldots||SIG(m_k).$$

   Show that given any single message $m \in M_k$, and a signature $SIG_1(m)$ we can find another message $m_0$ for which it is possible to calculate $SIG_1(m_0)$ without knowing the secret signature key of $SIG$.

   (b) We define a signature algorithm $SIG_2$, which given $m^* \in M_k$, divides $m^*$ into $2k$ blocks of $\ell/2$ bits each and signs $m^* = m_1||m_2\ldots||m_{2k}$ as:

   $$SIG_2(m^*) = SIG(1||m_1)||SIG(2||m_2)||\ldots||SIG(2k||m_{2k})$$

   where $i||m_i$ means the concatenation of the number $i$ (represented in $\ell/2$ bits) with the block $m_i$. Is $SIG_2$ a secure signature algorithm?

   [4 Marks]

10. You are the Chief Cryptologist of ABCD Corp. Your organization has been contacted by a telecom company "Ghodafone" to print mobile recharge vouchers for low value denominations. Users can buy these vouchers from retail shops and recharge their prepaid phones by typing the voucher numbers (to be sent to the phone company via USSD codes). Assuming that the phone company allows users to type only alphanumeric characters in a USSD code, design a scheme which is efficient and secure from the point of view of the phone company.

    What kind of attacks you expect against the voucher codes, and how does your scheme prevent these? (Note: We do not consider attacks like data theft from servers. We are concerned only with design flaws and attacks on them.) [4 Marks]