COMPSCI 4CR3 - Applied Cryptography **Fall 2024**

Practice Problems

1) Let $s_6 = a_5 s_5 + \cdots + a_1 s_1$ represent a linear feedback shift register (LFSR) with coefficients $a_1 a_2 a_3 a_4 a_5 = 11001$ and initial value $s_1 s_2 s_3 s_4 s_5 = 01011$. Compute the next 5 bits generated by this LFSR.

2) As discussed in class, a pseudorandom number generator (PRNG) is considered secure if it is computationally hard to distinguish its output from a uniformly random sequence. Explain why a PRNG based on a linear feedback shift register (LFSR) is not secure.

3) Let $g : \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$, be a PRNG defined by $g(x) = (x^3 \bmod p, x^5 \bmod p)$. Is this PRNG secure? Explain. (You must investigate whether a sequence of pairs $\{g(x_i)\}$ can be distinguished from a sequence $\{(a_i, b_i)\}$ where a_i and b_i are uniformly random numbers.)

4) Which of the following statements are true regarding AES:

(a) It is a bit-oriented cipher.

(b) It has fast software implementations.

(c) The Diffusion Layer is not invertible.

(d) The number of rounds depends on the key size.

(e) The arithmetic in AES, such as multiplication, is integer arithmetic.

(f) There are no known subexponential attacks against AES.

5) Let $u \in \mathbb{Z}_p^n$ be a fixed vector of length n with entries in $\mathbb{Z}_p$. Define a hash function $f_u : \mathbb{Z}_p^n \to \mathbb{Z}_p$ by $f_u(v) = \langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n \bmod p$. Is this hash function collision-resistant? Explain.

6) Let h_1 and h_2 be two collision resistant hash functions. Define $g(x) = h_1(h_2(x))$. Is g collision resistant? Explain.

7) Suppose $h : \{0,1\}^* \to \{0,1\}^n$ hash function that is preimage resistant and pseudorandom, i.e., the distribution of the output of h is close to uniform. Let $n = 128$, so the output of h is 16 bytes. We are looking for an input x such that the third 32 bits of $h(x)$ are

$$11100011100100011001011100110011.$$

In other words, we seek x such that $h(x) = y$, where

$$y = ab11100011100100011001011100110011cd,$$

and a, b, c, and d are arbitrary 32-bit strings. How many inputs, in the worst case, would we need to try to find such a y?

8) Let p be a large prime such that 7 does not divide $p-1$. Define the function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by $f(x) = x^7 \bmod p$. Is f a one-way function? Explain.

9) Let $r_0 = 112$ and $r_1 = 86$. Use the extended Euclidean algorithm to find s and t such that $sr_0 + tr_1 = \gcd(r_0, r_1)$.

10) Which of the following is not a generator for $\mathbb{Z}_{953}^{\times}$?

(a) 602

(b) 746

(c) 780

(d) 94

11) Let G be a finite cyclic group of size N, and let $g \in G$ be a generator. Suppose Trudy has access to an oracle that can solve the computational Diffie-Hellman problem, i.e., for any $1 \leq x, y < N$, given g^x and g^y, Trudy can efficiently compute g^{xy} by calling the oracle. Can Trudy solve the following problem efficiently:

$$\text{given } g^x \text{ and } n \in O(\log(N)), \text{ compute } g^{x^n+3x^2+x+5}.$$

12) Let $p = 953$ be a prime number. In the Elgamal signature scheme, Trudy has decided to forge a signature by writing a brute-force algorithm that tries all possible ephemeral keys. How many trials ephemeral keys does he have to try?

(a) Less than 219

(b) Less than 384

(c) More than 410

(d) More than 412

13) Let $(n, e) = (493, 205)$ be the public key in the RSA signature scheme. Which of the following is a valid message-signature pair?

(a) $(32, 16)$

(b) $(6, 415)$

(c) $(53, 83)$

(d) $(112, 45)$

14) Let $S = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme that is existentially unforgeable. Recall that in an existential forgery attack, the attacker constructs a new message-signature pair (m, s), where m has never been previously signed by the legitimate signer. Consider the following new signature scheme $S' = (\mathsf{Gen}, \mathsf{Sig}', \mathsf{Ver}')$ based on S, where Sig' and Ver' are defined as follows:

- $\mathsf{Sig}'(m, k_{pr})$: Choose a random $r \leftarrow \{0,1\}^n$, output $(r, \mathsf{Sig}(k_{pr}, m \oplus r), \mathsf{Sig}(k_{pr}, r))$.

- $\mathsf{Ver}'(m, k_{pub}, (r, s_1, s_2))$: Output "accept" if and only if

$$\mathsf{Ver}(k_{pub}, m \oplus r, s_1) = \mathsf{Ver}(k_{pub}, r, s_2) = \text{“accept”}.$$

Is S' a secure signature scheme? If so, justify your answer; otherwise, give an attack.

15) Briefly explain why the Discrete Logarithm Problem (DLP) over the group of points on an elliptic curve is more widely used than the DLP over the cyclic group $\mathbb{Z}_p^\times$.

16) In the DSA signature scheme, the public values are (p, q, α), where α is a generator of a subgroup of $\mathbb{Z}_p^\times$ of order q. Is it safe to fix these public values once and for all, so that everyone in the world uses them? Explain.

17) Suppose the public primes for the DSA signature scheme are $p = 2089$ and $q = 29$. Which of the following is a public key β for these parameters?

(a) 774

(b) 1762

(c) 1189

(d) 512

18) Let $h : \{0,1\}^* \to \{0,1\}^{100}$ be a preimage resistant hash function. Suppose you have a machine M that can compute 2^{30} hashes per second. Using M, approximately how long does it take to find a collision, with probability at least $1/2$, for h?

(a) 35 million years

(b) 15 days

(c) 1 year

(d) 10 years

19) Consider the curve $E : y^2 = x^3 + x + 2$ over $\mathbb{Z}_{11}$.

(a) Is this an elliptic curve? (Recall that the coefficients a and b must satisfy a certain condition.)

(b) The order of the group of points on E is 16. What is the order of the point $P = (8, 4) \in E$?

20) The parameters of a DSA scheme are given by $p = 59$, $q = 29$, $\alpha = 3$, and Bob's private key is $d = 23$. Show the process of signing (by Bob) and verification (by Alice) for the following hashed messages $h(x)$ and ephemeral keys k_E:

(a) $h(x) = 17$, $k_E = 25$

(b) $h(x) = 2$, $k_E = 13$