Principles of Information Security

Problem Set - 1

January 2026

Instructions

This Problem Set is provided purely for practice and does not require submission. Each problem is assigned a total of 10 points. Most problems are directly solvable, and all of them are solvable using AI.

During the exam, if a student is unable to solve a particular problem, they may explicitly write **"I DON'T KNOW"** along with a one-line description of the specific part they do not know or are stuck at; in this case, the student will be awarded 10% points for that problem. Leaving a problem unanswered without such a statement or description (rationale) will result in 0 points. For problems consisting of multiple sub-parts, writing the "I DON'T KNOW" statement anywhere within the problem will result in the entire problem being graded 10%, regardless of the correctness of any other sub-parts.

Note, this policy is only to be used as a **last resort** once you have exhausted all techniques in your skill set. We do not recommend relying on it while you are preparing.

Problem 1

A company designs a proprietary encryption system for protecting internal communications. Initially, both the encryption algorithm and the secret key are known only to the company. After several years of deployment, detailed documentation of the algorithm is leaked publicly, but the secret keys remain unknown.

(a) Assume that the system faces a successful attack shortly after the algorithm is revealed, even though the keys are still secret. What does this suggest about the original design assumptions?

(b) Based on the above scenario, state a general design guideline for cryptographic systems regarding which components may be assumed public and which must remain secret.

(c) Explain and differentiate between forward and backward secrecy.

Problem 2

Using your experience in security definitions, provide a definition for perfect pseudo-random generators $G : \{0,1\}^n \to \{0,1\}^{n+1}$. Furthermore, prove that such perfect PRGs do not exist.

Problem 3

Prove the following are hard-core predicates for DLP ($f(x) = g^x \bmod p$) in $\mathbb{Z}_p^*$ for a prime p, if $(p-1) = s.2^r$ for some odd s:

(a) the msb

(b) the $(r+1)^{\text{th}}$ lsb (that is, the bit that says if $x \bmod 2^{r+1}$ is $\geq 2^r$).

Using any of these, design a provably secure PRG assuming DLP is hard in $\mathbb{Z}_p^*$.

Problem 4

Consider a modification of the substitution cipher, where instead of applying only the substitution, we first apply a substitution and then apply a shift cipher on the substituted values. Give a formal description of this scheme and show how to break the substitution and shift cipher.

Problem 5

Assume the adversary has the ability to obtain ciphertexts for arbitrary plaintexts, i.e., it can choose a message and receive an encryption of the message without knowing the secret key. Attacks that leverage this information are known as chosen plaintext attacks.

(a) Using chosen plaintext attacks, show how to learn the secret key for the shift, substitution, and Vigenère ciphers. Your attacks should each use only a single plaintext. What is the smallest plaintext length that suffices for each attack?

(b) For the Vigenère cipher, please consider two cases:

(i) when the period t is known;

(ii) when the period t is unknown but an upper bound t_{max} on t is known. For the latter case, an asymptotic analysis of the required plaintext length suffices, i.e., an upper bound on the required plaintext length.

Problem 6

Negligible or not?

(a) Let $f, g : \mathbb{N} \to \mathbb{R}$ be negligible functions, let $p : \mathbb{N} \to \mathbb{R}$ be a polynomial such that $p(n) > 0$ for all $n \in \mathbb{N}$.

(i) Define $h(n) = f(n) + g(n)$.

(ii) Define $h(n) = f(n) \cdot p(n)$.

(iii) $f(n) := f'(n) \cdot p(n)$ for some negligible function $f'(n)$ and some polynomial function $p(n)$. Is such a $f(n)$ always negligible?

(b) For each of the following functions below, either prove or disprove that it is negligible.

(i) $f(n) := 1/2^{100 \log n}$

(ii) $f(n) := 1/(\log n)^{\log n}$

(iii) $f(n) = n^{-100} + 2^{-n}$

(iv) $f(n) = 1.01^{-n}$

(v) $f(n) = 2^{-(\log n)^2}$

(vi) $f(n) = 2^{-\sqrt{n}}$

(vii) $f(n) = 2^{-\sqrt{\log n}}$

(viii) $f(n) = \frac{1}{(\log n)!}$

Problem 7

Let p be a prime and consider the discrete logarithm problem in the group $\mathbb{F}_p^*$, which has order $p-1$. Explain which primes p are unsuitable for discrete-logarithm–based cryptography due to the Pohlig–Hellman attack. In particular, characterize the factorization of $p-1$ that makes the discrete logarithm problem efficiently solvable.

Problem 8

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme in which the key-generation algorithm Gen outputs a key K according to an arbitrary (not necessarily uniform) distribution over some finite key space $\mathcal{K}$. For any message m, let

$$C = \mathsf{Enc}(K, m),$$

where the probability is taken over the randomness of Gen (and Enc, if randomized).

Prove that there exists an equivalent encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ with a (possibly different) key space $\mathcal{K}'$ such that:

1. Gen' samples a key uniformly from $\mathcal{K}'$; and
2. for all messages m and ciphertexts c,

$$\Pr[C = c \mid M = m] = \Pr[C' = c \mid M = m],$$

   where $C' = \mathsf{Enc}'(K', m)$ and the probability is over the randomness of Gen' (and Enc', if applicable).

Problem 9

PRG or not? Let $G : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ be a pseudorandom generator (PRG). For each part below, either prove or disprove that $G' : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ is necessarily a PRG no matter which PRG G is used.

(a) $G'(x) := G(\pi(x))$ where $\pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is any $poly(n)$-time computable bijective function. (You may not assume that π^{-1} is $poly(n)$-time computable.)

(b) $G'(x||y) := G(x||x \oplus y)$, where $|x| = |y| = n$.

(c) $G'(x||y) := G(x||0^n) \oplus G(0^n||y)$, where $|x| = |y| = n$.

(d) $G'(x||y) := G(x||y) \oplus (x||0^{n+1})$, where $|x| = |y| = n$.

Problem 10

An encryption scheme (Gen, Enc, Dec) over message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is said to be 2-time perfectly secure if for any $(m_1, m_2) \in \mathcal{M} \times \mathcal{M}$ and $(m_1', m_2') \in \mathcal{M} \times \mathcal{M}$ such that $m_1 \neq m_2$ and $m_1' \neq m_2'$ and for any $c_1, c_2 \in \mathcal{C}$ the following holds:

$$Pr[Enc(K, m_1) = c_1 \wedge Enc(K, m_2) = c_2] = Pr[Enc(K, m_1') = c_1 \wedge Enc(K, m_2') = c_2]$$

Consider the following encryption scheme for the message space $\mathbb{Z}_{23}$:

- Gen: Sample two elements $a \leftarrow \mathbb{Z}_{23}$ and $b \leftarrow \mathbb{Z}_{23}$.
- $Enc((a, b), m)$: Output $c = a \cdot m + b \pmod{23}$.

- $Dec((a,b),c)$: Compute $m = (c - b) \cdot a^{-1} \pmod{23}$ if a is invertible. Otherwise, output error.

Show the following:

(a) Prove that for any message $m \in \mathbb{Z}_{23}$, $Pr[Dec(K, Enc(K,m)) = m] = \frac{22}{23}$.

(b) Prove that this is 2-time secure.

Problem 11

The following questions concern the message space $\mathcal{M} = \{0,1\}^{\leq \ell}$, the set of all nonempty binary strings of length at most ℓ.

(a) Consider the encryption scheme in which Gen chooses a uniform key from $\mathcal{K} = \{0,1\}^{\ell}$, and $\mathsf{Enc}_k(m)$ outputs $k_{|m|} \oplus m$, where k_t denotes the first t bits of k. Show that this scheme is not perfectly secret for message space $\mathcal{M}$.

(b) Design a perfectly secret encryption scheme for message space $\mathcal{M}$.

Problem 12

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF). For the functions f' below, either prove that f' is a PRF (for all choices of f), or prove that f' is not a PRF.

(a) $f'_k(x) := f_k(0||x)||f_k(1||x)$.

(b) $f'_k(x) := f_k(0||x)||f_k(x||1)$.

Problem 13

Let F be a PRF defined over (K, X, Y), where $X = \{0, \dots, N-1\}$ and $Y = \{0,1\}^n$, where N is super-poly. For poly-bounded $l \geq 1$, consider the PRF F' defined over (K, X, Y^l) as follows:

$$F'(k,x) := (F(k,x), F(k, x+1 \pmod{N}), \dots, F(k, x+l-1 \pmod{N}))$$

(a) Show that F' is a weakly-secure PRF.

(b) Prove that randomized counter mode is CPA secure.

Problem 14

Assume that one-way functions exist. $b : \{0,1\}^* \to \{0,1\}$ is a hard-core predicate of a one-way function $f(\cdot)$ if $b(x)$ is efficiently computable given x and there exists a negligible function such that for every PPT adversary A and for every n: $Pr[A(f(x)) = b(x)] \leq \frac{1}{2} + \nu(n)$.

(a) Construct a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ for input $x = (x_1, x_2, \dots, x_n)$ such that the first bit x_1 is not hardcore.

(b) A polynomial time-computable predicate $b : \{0,1\}^n \to \{0,1\}$ is called a universal hard-core predicate if for every one-way function $f : \{0,1\}^n \to \{0,1\}^m$, b is hardcore. Prove that there is no universal hardcore predicate.

(c) Could there be a one-way function f for which none of the individual bits of the input are hardcore? Construct a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ for which none of the predicates $b_i(x_1, \dots, x_n) = x_i$ are hardcore.

Problem 15

Suppose (Gen, Enc, Dec) is a CPA-secure encryption scheme that encrypts messages belonging to a field $\mathcal{F}$. Construct a new encryption scheme as follows:

- $Gen_1(1^n)$ samples $k' \leftarrow Gen(1^n)$, then samples p, a random degree-d polynomial over $\mathcal{F}$. The key $k = (k', p)$.
- $Enc_1(k, m) = Enc(k', m)||p(m)$.
- $Dec_1(k, c)$ runs $Dec(k', \cdot)$ on the first part of the ciphertext.

In the CPA security experiment, what is the minimum number of queries to the Enc oracle that are needed to break the CPA security of the scheme (Gen_1, Enc_1, Dec_1)?

Problem 16

Give complete details of how to construct Y from X where:

(a) X = One-way permutation, Y = pseudorandom generator.

(b) X = pseudorandom generator, Y = one-way function.

(c) X = pseudorandom generator, Y = pseudorandom function.

Problem 17

Let F be a length-preserving pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme is EAV-secure and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0, 1\}^n$.) Explain your answer in each case.

1. To encrypt $m \in \{0, 1\}^{n+1}$, choose uniform $r \in \{0, 1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m\rangle$.
2. To encrypt $m \in \{0, 1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
3. To encrypt $m \in \{0, 1\}^{2n}$, parse m as $m_1\|m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0, 1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r + 1)\rangle$.

Problem 18

Show that the existence of one-way functions implies $\mathsf{P} \neq \mathsf{NP}$. Assume that $\mathsf{P} \neq \mathsf{NP}$. Show that there exists a function f that is: computable in polynomial time, hard to invert in the worst case (i.e., for all probabilistic polynomial-time algorithms A,

$$\Pr_{x \leftarrow \{0,1\}^n}[f(A(f(x))) = f(x)] \neq 1),$$

but *not* one-way.

Problem 19

Let $\mathcal{F} : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n$ be a PRF and let $\mathcal{G}(k, (x, y)) = \mathcal{F}(k, x) \oplus \mathcal{F}(k, y)$. Prove that $\mathcal{G}$ is not a PRF.

Problem 20

What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext $c_1, c_2, c_3, \dots$ is received as $c_1, c_3, \dots$) when using the CBC, OFB, and CTR modes of operation? Also, consider a variant of CTR mode where a uniform $IV \in \{0,1\}^n$ is chosen and the ith ciphertext block is computed as $c_i := m_i \oplus F_k(IV + i)$. Prove that this variant is CPA-secure. What concrete-security bound do you obtain?

Problem 21

Let $\mathcal{F} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF. Prove that $\mathcal{H}(k, x) = \mathcal{F}(k, x) \oplus x$ is also a PRF.

Problem 22

When using the one-time pad with the key $k = 0^\ell$, we have $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., to have Gen choose k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme still perfectly secret? Explain.

Problem 23

Let (Gen, Enc, Dec) be a CPA-secure encryption scheme. Construct (Gen_1, Enc_1, Dec_1):

- $Gen_1(1^n)$: $k \leftarrow Gen(1^n)$.
- $Enc_1(k, m)$: Sample $r \leftarrow \{0,1\}^n$ uniformly. $c_0 := Enc(k, r)$, $c_1 := r \oplus m$. Output $c = (c_0, c_1)$.

(a) Fill in the decryption algorithm $Dec_1(k, (c_0, c_1))$ for correct decryption.

(b) Prove that (Gen_1, Enc_1, Dec_1) satisfies CPA security.

Problem 24

Prove that no encryption scheme can satisfy the following definition of perfect secrecy for two messages: For all distributions over $\mathcal{M} \times \mathcal{M}$, all $(m_1, m_2) \in \mathcal{M} \times \mathcal{M}$ and all $(c_1, c_2) \in \mathcal{C} \times \mathcal{C}$ where $Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = Pr[M_1 = m_1 \wedge M_2 = m_2]$$

Problem 25

(a) Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

(b) Say CBC-mode encryption is used with a block cipher having a 256-bit key and 128-bit block length to encrypt a 1024-bit message. What is the length of the resulting ciphertext?

Problem 26

Define functions $g(n) = 2^{-f(n)}$.

(a) Prove that if $f(n) = \omega(\log n)$, then $g(n)$ is negligible.

(b) Prove that if $f(n) = O(\log n)$, then $g(n)$ is non-negligible.

Problem 27

Let f be a length-preserving one-way function. Prove or provide a counterexample for the one-wayness of:

(a) $f_0(x) = f(f(x))$

(b) $f_1(x, y) := f(x)||f(x \oplus y)$

(c) $f_2(x) := (f(x)||x_{[1:\log|x|]})$

(d) $f_3(x) := f(x)_{[1:|x|-1]}$

(e) $f_4(x) := f(x) \oplus x$

Problem 28

Let $\mathcal{F}_n$ be a Pseudo-Random Function family. Prove either that $f'_k \in \mathcal{F}'_n$ is a PRF or provide an attack for it:

(a) $f'_k(x, y) = f_k(x) \oplus f_k(y)$

(b) $f'_k(x, y) = f_k(x \oplus y)$

(c) $f'_k(x, y) = f_{k \oplus x}(y)$

(d) $f'_k(x, y) = f_{f_k(x)}(y)$