試 験 科 目 名 Subject
科目名　情報学 (英文)　Informatics

受験番号 Examniee's Number	M

広島大学大学院先進理工系科学研究科（博士課程前期）入学試験問題（2025年10月入学及び2026年4月入学）
Entrance Examination for Master's Course (October 2025 Enrollment and April 2026 Enrollment),
Graduate School of Advanced Science and Engineering

問題 1（Question1）

RFC 5280 は、公開鍵基盤（Public Key Infrastructure, PKI）に基づくデジタル証明書および証明書失効リスト（Certificate Revocation List, CRL）の形式と検証方法を定義しており、これらは安全な通信や鍵交換において重要な役割を果たす。PKI におけるデジタル証明書の発行およびその信頼性維持に関して、以下の問いに答えよ。

(1) 以下の記述は、デジタル証明書の発行手順の概要である。空欄①～⑤に当てはまる最も適切な語句を記述せよ。

エンティティ A は、まず【 ① 】と公開鍵のペアを生成し、【 ② 】を作成して、【 ③ 】に提出する。【 ③ 】は A の情報を検証し、【 ④ 】を発行し、署名して A に返却する。その後、A は【 ⑤ 】をエンティティ B に提示して、自身の身元と鍵情報を信頼可能な形で伝える。

(2) PKI において、認証局（Certificate Authority, CA）が侵害（不正アクセスや悪用など）された場合、攻撃者が実行可能となる深刻なセキュリティ上の脅威を 2 つ挙げ、それぞれについてその影響とリスクを説明せよ。
なお、ここでいう「侵害」とは、攻撃者が認証局の正規の権限を不正に行使できる状態を指す。

RFC 5280 defines the format and validation procedures for a digital certificate and a Certificate Revocation List (CRL) based on the Public Key Infrastructure (PKI). These components play an essential role in secure communication and key exchange. Answer the following questions regarding the issuance and trust management of a digital certificate in PKI.

(1) The following description outlines the procedure for issuing a digital certificate. Fill in blanks ① to ⑤ with the most appropriate terms.

An entity A first creates【 ① 】 and a public key, then generates【 ② 】 and submits it to【 ③ 】. 【 ③ 】 verifies information of A, issues【 ④ 】, and returns it to A with a signature. Later, A presents【 ⑤ 】 to an entity B to convey its identity and key information in a trustworthy manner.

(2) In PKI, if the Certificate Authority (CA) is compromised (e.g., unauthorized access or abuse of authority), show two serious security threats that an attacker could exploit, and explain the impact and associated risk of each threat.
Note that "compromised" here refers to a situation in which the attacker can illegally exercise the legitimate authority of the CA.

試 験 科 目 名 Subject
科目名　情報学 (英文)　Informatics

問題 2（Question2）

以下は、メッセージの完全性および認証を確保するためのハッシュ関数と HMAC（Keyed-Hash Message Authentication Code）の仕組みについて、RFC 2104 の記述に基づいてまとめたものである。以下の問いに答えよ。

(1) 以下の文章の空欄①～⑥に当てはまる最も適切な語句を記述せよ。

送信者は、共有鍵 K とメッセージ M を使って【 ① 】を生成する。このとき、暗号学的【 ② 】関数を用いる。このように生成された【 ① 】は、メッセージとともに受信者に送信される。受信者は同じ【 ③ 】と【 ④ 】を用いて再計算を行い、受信した【 ① 】と一致すれば、メッセージが改ざんされていないことを確認できる。この仕組みは、ハッシュ関数の【 ⑤ 】と【 ⑥ 】耐性に基づいている。

(2) メッセージ認証コード（MAC）を用いた改ざん検出の仕組みについて説明せよ。説明には、以下の前提条件を踏まえた上で、なぜ改ざんが検出できるのかを技術的理由と攻撃者の制約の観点を含めること。解答は 200 字程度を目安とすること。

【前提条件】

- 通信路上に攻撃者が存在し、メッセージを任意に改ざんできると仮定する
- 攻撃者は共有鍵 K を知らないものとする

The following description outlines mechanisms of hash functions and HMAC (Keyed-Hash Message Authentication Code) to ensure message integrity and authentication, based on RFC 2104. Answer the following questions.

(1) Fill in blanks ① to ⑥ with the most appropriate terms.

The sender generates【 ① 】using a shared key K and message M. At this point, a cryptographic【 ② 】function is used in this process. The【 ① 】generated in this way is sent to a receiver with the message. The receiver recomputes using the same【 ③ 】and【 ④ 】, and if the result matches the received【 ① 】, it can confirm that the message has not been tampered with. This mechanism is based on the【 ⑤ 】and【 ⑥ 】resistance of the hash function.

(2) Explain the mechanism of tamper detection using message authentication codes (MAC). In your explanation, assume the following assumptions and include technical reasons and attackers' constraints as to why tampering can be detected. Answer should be approximately 200 characters.

【Assumptions】

- Assume that an attacker on the communication channel can arbitrarily intercept messages.
- Assume that the attacker does not know the shared secret key K.

試 験 科 目 名 Subject
科目名　情報学 (英文)　Informatics

問題 3（Question3）

信頼できる計算環境（Trusted Execution Environment, TEE）に関して、それぞれ 200 文字程度で次の問に答えよ。

(1) TEE を利用する利点を 2 つ挙げ、それぞれの内容を説明せよ。

(2) TEE の限界を 2 つ挙げ、それぞれの内容を説明せよ。

(3) TEE におけるリモートアテステーション（Remote Attestation）について簡潔に説明せよ。

(4) クラウドサービスなどの具体的な利用シナリオを 1 つ挙げ、TEE とリモートアテステーションがどのように機能するかを説明せよ。

(5) 上記（4）のシナリオにおけるセキュリティ上の利点とリスクを 1 つずつ挙げて説明せよ。

Answer the following questions regarding the Trusted Execution Environment (TEE). Each answer should be approximately 200 characters.

(1) Show two advantages of using TEE, and explain them.

(2) Show two limitations of TEE, and explain them.

(3) Explain Remote Attestation in TEE briefly.

(4) Show one specific use case (e.g., cloud service), and explain how TEE and Remote Attestation work.

(5) Explain one security advantage and one risk in the above scenario (4).

試 験 科 目 名 Subject
科目名　情報学 (英文)　Informatics

問題 4 (Question4)

ID ベース暗号 (Identity-Based Encryption, IBE) に関して、それぞれ 200 文字程度で次の問いに答えよ。

(1) IBE と公開鍵基盤 (PKI) のアーキテクチャ上の主要な違いを簡潔に説明せよ。

(2) IBE における鍵預託問題 (key escrow problem) とは何かを説明せよ。

(3) IBE における鍵預託問題に対処するための技術的アプローチの一例を挙げ、その課題点を簡潔に説明せよ。

Answer the following questions regarding Identity-Based Encryption (IBE). Each answer should be approximately 200 characters.

(1) Explain the main architectural difference between IBE and Public Key Infrastructure (PKI) briefly.

(2) Explain the key escrow problem in IBE.

(3) Show one technical approach to address the key escrow problem in IBE, and explain its limitations briefly.

解答例（Sample Answer）

試 験 科 目 名 Subject
情報学 Informatics

問題 1 解答例

(1) エンティティ A は、まず【①秘密鍵】と公開鍵のペアを生成し、【②証明書署名要求】を作成して、【③認証局】に提出する。【③認証局】は A の情報を検証し、【④デジタル証明書】を発行し、署名して A に返却する。その後、A は【⑤デジタル証明書】をエンティティ B に提示して、自身の身元と鍵情報を信頼可能な形で伝える。

(2) 脅威 1：偽の証明書の発行：

【影響】攻撃者が侵害された CA の秘密鍵を用いて、任意のドメイン名や個人・組織の名義で偽のデジタル証明書を発行できる。

【リスク】この偽証明書により、攻撃者は正規のウェブサイトになりすまし、中間者攻撃やフィッシング攻撃を実行できる

脅威 2：証明書失効リストやデジタル証明書の状態確認プロトコルの偽装：

【影響】攻撃者が証明書失効リスト（CRL）や OCSP（Online Certificate Status Protocol）レスポンスを偽造することで、失効済みの証明書を有効に見せかけることができる。

【リスク】ユーザーが偽証明書を信頼し続けることで、長期間にわたり機密情報が漏洩したり、不正アクセスが継続したりする。

問題 1 出題意図

(1) PKI の基本手順の正確な理解を確認するため。

(2) PKI の信頼モデルにおける単一障害点である認証局の侵害がセキュリティ全体に与える影響の理解を確認するため。

問題 2 解答例

(1) 送信者は、共有鍵 K とメッセージ M を使って【①メッセージ認証コード】を生成する。このとき、暗号学的【②ハッシュ】関数を用いる。このように生成された【①メッセージ認証コード】は、メッセージとともに受信者に送信される。受信者は同じ【③共有鍵 K】と【④メッセージ M】を用いて再計算を行い、受信した【①メッセージ認証コード（MAC）】と一致すれば、メッセージが改ざんされていないことを確認できる。この仕組みは、ハッシュ関数の【⑤一方向性】と【⑥衝突】耐性に基づいている。

(2) メッセージ認証コード（MAC）による改ざん検出は、共有鍵 K の秘匿性に依存する。送信者は、共有鍵 K とメッセージ M を暗号学的ハッシュ関数に入力し MAC を生成する。この MAC は、メッセージの完全性と認証情報として送信される。通信路上でメッセージが改ざんされても、攻撃者は正しい共有鍵 K を知らないため、有効な MAC を生成できない。受信者は、受信したメッセージと自身の共有鍵 K で MAC を再計算し、受信した MAC と比較する。一致しなければ、改ざんを確実に検出できる。

問題 2 出題意図

(1) HMAC の動作原理の理解を確認するため。

(2) MAC の安全性の本質を技術的観点で説明できることを確認するため。

問題 3 解答例

(1) 1つ目の利点は、OSやハイパーバイザが信頼できなくても、隔離された環境で安全に処理できる点である。攻撃者が管理者権限を取得しても、TEE内の秘密情報にはアクセスできない。2つ目は、暗号鍵や認証トークンなどの機密データをTEE内で安全に生成・保持・使用でき、従来のソフトウェアベースの保護よりも高い耐改ざん性を実現できる点である。

(2) 1つ目の限界は、ハードウェアの脆弱性に依存する点であり、TEEが実装されたCPUにバグがある場合、TEE全体が危殆化するリスクがある。2つ目は、サイドチャネル攻撃への脆弱性であり、実行時間や電力消費などの観測から秘密情報が漏洩する可能性がある。特に、TEEを提供するハードウェアの1つであるIntel SGXはこれまでに複数のサイドチャネル攻撃が報告されている。

(3) リモートアテステーションとは、TEE上で実行されるコードの整合性や信頼性を、外部の検証者が確認できる仕組みである。TEEは、実行されるプログラムのハッシュ値を計算し、それに対する署名付きの証明書を生成する。これを通信相手に送信することで、受信側は信頼できるコードがTEE上で動作していることを確認でき、なりすましや改ざんを防止できる。

(4) 医療機関がクラウド上で個人健康情報を処理する際、TEEを用いてデータの復号・分析を安全に実行できる。利用者はリモートアテステーションにより、クラウドサービス事業者のTEE内で想定通りのコードが実行されていることを確認できる。これにより、クラウド事業者がデータにアクセスできない状態で、分析処理が安全に行える。

(5) 利点は、クラウド事業者がOSやハードウェアレベルで信頼できなくても、TEEにより医療データの機密性と実行の正当性を担保できる点である。リスクとしては、TEEに依存するため、そのハードウェアやTEE内で動作するプログラムに未知の脆弱性があった場合、外部に漏れないはずのデータが攻撃者に奪取される可能性がある。設計や更新ミスによるリスクにも注意が必要である。

問題3出題意図

(1) TEEが提供する基本的なセキュリティ機能（分離、データ保護、コード検証など）についての正確な理解と、実用的な視点からの利点を記述できるかを確認するため。

(2) TEEの限界やリスク（脆弱性依存、機能制約など）を把握しており、過信せずに設計できるバランス感覚があるかを確認するため。

(3) TEEと併せて重要な機能であるリモートアテステーションについて、仕組みと目的を簡潔に正確に説明できるかを確認するため。

(4) TEEとリモートアテステーションが用いられる具体的な実装シナリオを自ら考え、それぞれの役割と連携について説明できるかを確認するため。

(5) 考案したシナリオにおいて、セキュリティ強化の能力とリスクを評価の能力を確認するため。

問題4解答例

(1) IDベース暗号（IBE）では、利用者の識別子（例：メールアドレス）自体が公開鍵として機能し、秘密鍵は信頼された鍵生成センター（KGC）によって生成されるため、証明書の配布が不要である。一方、公開鍵基盤（PKI）では、各利用者が公開鍵と秘密鍵を生成し、認証局（CA）が公開鍵の正当性を証明する証明書を発行する必要がある。これにより、証明書の管理や検証が必要となるが、KGCのような中央集権的な機関を必要としない。

(2) IBEでは、すべての秘密鍵がKGCによって生成される。このため、KGCは任意のユーザーの秘密鍵を再生成可能であり、通信内容を復号する能力を持つ。このようにKGCに通信の盗聴やなりすましが理論的に可能となってしまう問題を「鍵預託問題」と呼ぶ。ユーザーは自分の鍵を完全に管理できないという点で、従来のPKIよりも信頼性に課題がある。

(3) 鍵預託問題への対策として、分散型KGC（複数の鍵生成機関による秘密鍵の分割生成）が提案されている。各機関が一部の秘密鍵を生成し、最終的な鍵はユーザー自身が構成する。この方法により単一機関への依存を低減できるが、機関間の同期・信頼関係の構築、鍵復元の失敗リスクなど運用上の課題がある。

問題4出題意図

(1) IBE と PKI の構造的な違いを理解しているかを確認するため。
(2) IBE の根本的な課題である鍵預託問題を正しく説明できるかを確認するため。
(3) 現実的な対策とその限界を具体的に把握しているかを確認するため。

Question1 Sample Answer

(1) Entity A first generates【①Private Key】 and a public key, then creates【②Certificate Signing Request (CSR)】 and submits it to【③Certification Authority (CA)】. 【③Certification Authority (CA)】 verifies information of A, issues 【④Digital Certificate】, and returns it to A with a signature. Later, A presents【⑤Digital Certificate】 to an entity B to convey its identity and key information in a trustworthy manner.

(2) Threat1: Issuance of fake certificates:
[Impact] Attackers can use the compromised CA's private key to issue fraudulent digital certificates for any domain or entity.
[Risk] This enables attackers to impersonate legitimate websites and conduct Man-in-the-Middle (MITM) or phishing attacks.

Threat2: Falsification of Certificate Revocation Lists or Digital Certificate Status Protocols:
[Impact] Attackers can forge Certificate Revocation Lists (CRLs) or OCSP (Online Certificate Status Protocol) responses to make revoked certificates appear valid.
[Risk] Users may continue to trust fake certificates, leading to prolonged data breaches or unauthorized access.

Question1 Purpose of the Question

(1) To evaluate accurate understanding of the fundamental procedures of PKI.
(2) To evaluate understanding of how the compromise of the Certificate Authority (CA), as a single point of failure in the PKI trust model, affects the overall security.

Question2 Sample Answer

(1) The sender generates【①Message Authentication Code (MAC)】 using a shared key K and message M. At this point, a cryptographic【②Hash】 function is used in this process. The 【①Message Authentication Code (MAC)】 generated in this way is sent to a receiver with the message. The receiver recomputes using the same【③Shared Key K】 and【④Message M】, and if the result matches the received【①Message Authentication Code (MAC)】, it can confirm that the message has not been tampered with. This mechanism is based on the【⑤One-wayness】 and【⑥Collision】 resistance of the hash function.

(2) Tamper detection using Message Authentication Code (MAC) depends on the secrecy of the shared key K. The sender inputs the shared key K and message M into a cryptographic hash function to generate a MAC. This MAC is sent as integrity and authentication information for the message. Even if the message is tampered with on the communication channel, the attacker cannot generate a valid MAC because they do not know the correct shared key K. The receiver recalculates the MAC using the received message and their own shared key K, and compares it with the received MAC. If they do not match, tampering can be reliably detected.

Question2 Purpose of the Question

(1) To evaluate understanding of how HMAC works.
(2) To evaluate ability to explain the essence of MAC security from a technical perspective.

Question3 Sample Answer

(1) The first advantage is that data can be securely processed in an isolated environment, even if the OS or hypervisor cannot be trusted. Even if an attacker gains administrator privileges, they cannot access the secret information within the TEE. The second advantage is that confidential data such as encryption keys and authentication tokens can be safely generated, stored, and used within the TEE, providing stronger tamper resistance compared to conventional software-based protections.

(2) The first limitation is that TEE security depends on hardware, meaning that if the CPU implementing the TEE has a vulnerability or bug, the entire TEE may become compromised. The second limitation is its susceptibility to side-channel attacks, where attackers may extract secret information by observing factors such as execution time or power consumption. In particular, side-channel attacks have been reported against Intel SGX, one of the hardware of TEE, in the past.

(3) Remote Attestation is a mechanism that allows an external verifier to confirm the integrity and trustworthiness of code running inside a TEE. The TEE calculates a hash value of the program being executed and generates a certificate signed with a secure key. By sending this certificate to the communicating party, the receiver can verify that the expected trustworthy code is running within the TEE, thereby preventing impersonation and tampering.

(4) When a healthcare organization processes personal health records (PHR) in the cloud, TEE can be used to securely perform data decryption and analysis. Through Remote Attestation, the user can verify that the expected code is running within the cloud service provider's TEE. This ensures that the analysis can be conducted safely, while the cloud provider remains unable to access the data.

(5) The advantage is that even if the cloud service provider is not trustworthy at the OS or hardware level, the TEE ensures both the confidentiality of medical data and the integrity of its execution. However, a potential risk lies in the dependency on TEE. If there are unknown vulnerabilities in the underlying hardware or in the program running within the TEE, data that should not be leaked to the outside may be stolen by attackers. It is also necessary to be aware of risks due to design and update errors.

Question3 Purpose of the Question

(1) To evaluate accurate understanding of the basic security functions provided by TEE (separation, data protection, code verification, etc.) and ability to explain their practical advantages.

(2) To evaluate understanding of the limitations and risks of TEE (vulnerability dependence, functional constraints, etc.) and the sense of balance to design without overconfidence.

(3) To evaluate ability to explain the mechanism and purpose of Remote Attestation, which is an important function alongside TEE.

(4) To evaluate ability to design specific implementation scenarios with TEE and Remote Attestation and to explain their respective roles and how they work together.

(5) To evaluate ability to assess both the security enhancements and risk within the proposed scenario.

Question4 Sample Answer

(1) In Identity-Based Encryption (IBE), a user's identifier (e.g., email address) functions directly as the public key, and the corresponding private key is generated by a trusted authority called the Key Generation Center (KGC). This eliminates the need to distribute digital certificates. In contrast, in a Public Key Infrastructure (PKI), users generate their own key pairs, and a Certificate Authority (CA) issues certificates to validate the authenticity of public keys. While this approach does not require a centralized key issuer like a KGC, it involves complex certificate management and validation processes.

(2) In IBE, all private keys are generated by the KGC, which means the KGC can regenerate any user's private key. This gives the KGC the theoretical ability to decrypt communications or impersonate users. This issue is known as the "key escrow problem." Users cannot fully manage their own keys, which poses a reliability problem compared to conventional PKI.

(3) A proposed solution to the key escrow problem is the use of distributed KGCs, where multiple key authorities each generate partial keys, and the user combines them to obtain the final private key. This approach reduces reliance on a single authority. However, it introduces operational challenges, such as coordinating between authorities, ensuring mutual trust, and handling key reconstruction failures in case of authority downtime or misbehavior.

Question4 Purpose of the Question

(1) To evaluate understanding of the structural difference between IBE and PKI.

(2) To evaluate ability to explain the key escrow problem, a fundamental issue in IBE.

(3) To evaluate understanding of practical solutions and their limitations regarding IBE's key escrow issue.