問題 B

ネットワークを介してメッセージ交換を行う際には，ネットワーク上での盗聴や改ざんを防ぐために，送信者がメッセージ（平文）を暗号化鍵（K_e）で暗号化や署名をして通信を行い，受信者が復号鍵（K_d）を用いて暗号文の復号や署名を検証する暗号化技法が良く用いられる．

K_e と K_d に異なる鍵を用いる公開鍵暗号方式には，以下の特徴がある．

送信者 A が，受信者 B の公開鍵 K_p^B を用いて暗号化した暗号文は，受信者 B が持つ私有鍵 K_s^B のみで復号できるため，ネットワーク上での盗聴を防ぐことができる．

一方，送信者 A が，送信者 A の私有鍵 K_s^A を用いた署名は，受信者 B が送信者 A の公開鍵 K_p^A を用いて検証することで，内容が改ざんされていないことが確認できる．

以下の問に答えよ．

(1) 公開鍵暗号方式の一つである RSA アルゴリズムを用いて “aa” から “ge” までの 161 種の英字列で構成されるメッセージを第三者が暗号化鍵 K_e=(53,161)で暗号化した暗号文を復号した元のメッセージを推定したい．以下の問に推定の過程とともに示せ．

ここで，RSA アルゴリズムでは，平文 M ($0 \le M < n$ を満たす整数) から暗号文 C を暗号化鍵 $K_e=(e,n)$ で生成するには $C = M^e \bmod n$ を用い，暗号文 C から平文 M を復号鍵 K_d=(d,n) で生成するには $M = C^d \bmod n$ が用いられる．n は，2 つの素数 p, q を用いて $n = p \cdot q$ として表され，d および e は，$L = (p-1)\cdot(q-1)$ として，$d \cdot e \bmod L = 1$ を満たす組合せから選ばれる．さらに，メッセージ及び暗号文は “aa”=0,…, “az”=25, “ba”=26,…, “ge”=160 と符号化して表現されていると考えよ．

(a) 暗号鍵 K_e に対応した復号鍵 K_d を推定せよ．

(b) 問(a)で推定した復号鍵 K_d を用いることで，暗号文 “ca, af, ad” を復号した元のメッセージを推定せよ．

(2) 次に，問(1) で述べた RSA アルゴリズムを用いてメッセージを暗号化することを考える．復号鍵を持たない第三者が元のメッセージを推定することが極端に難しくなるようにするためには，どうすれば良いか簡潔に答えよ．

(3) 送信者 A から受信者 B に対して，メッセージの内容が改ざんされていないことが確認でき，第三者には盗聴されない暗号文として送信するためには，送信者 A および受信者 B は，公開鍵暗号方式を用いたどの様な手法を用いれば良いか，その方式について述べよ．

(4) 第三者 X が，X の公開鍵 K_p^X を受信者 B の公開鍵と偽って送信者 A に伝えた場合，送信者 A が受信者 B 宛に生成した暗号文には，どのような危険性があるか述べよ．また，このような危険性を回避するためのアイデアについて述べよ．

Problem B

When we exchange messages through a network, cryptographic technologies are often used to encrypt or sign plain text messages using an encryption key (K_e) at the sender side and decrypt the ciphertext messages or verify the signature using a decryption key (K_d) at the receiver side to avoid eavesdropping and falsification.

The public key cryptography using two different keys for K_e and K_d has the following characteristics.

When sender A encrypts a plain text message with the public key of receiver B, K_p^B, the ciphertext message can be decrypted only with the private key of receiver B, K_s^B. It means that the original plain text message cannot be eavesdropped.

On the other hand, when sender A signs a plain text message with the private key of sender A , K_s^A, the signature can be verified with the public key of sender A, K_p^A, by receiver B. It means that the original plain text message is not falsified.

Answer the following questions.

(1) The RSA algorithm is a typical public key cryptographic technology. When a third-party encrypts 161 types of alphabetical messages from "aa" to "ge" using RSA with encryption key K_e=(53, 161), we would like to infer the original plain text messages from ciphertext messages. Answer the following questions with break process.

Here, in RSA, a plain text message M (M is an integer such that $0 \le M < n$) is encrypted to the ciphertext message C using encryption key $K_e = (e,n)$ as $C = M^e \bmod n$. A ciphertext message C is decrypted to the plain text message M using decryption key $K_d = (d,n)$ as $M = C^d \bmod n$. Here, n is computed using two prime numbers p and q as $n = p \cdot q$. Furthermore, d and e are selected so that $d \cdot e \bmod L = 1$, where $L = (p-1) \cdot (q-1)$. Assume that plain text messages and ciphertext messages are encoded as "aa"=0,..., "az"=25, "ba"=26,..., "ge"=160.

(a) Infer the decryption key K_d corresponding to encryption key K_e.

(b) Using decryption key K_d in Question (a), infer the original plain text messages of ciphertext messages "ca, af, ad".

(2) Suppose that we are the sender and convert messages using the RSA algorithm described in Question (1). We would like to make it extremely difficult for those who do not have the decryption key to infer the original plain text messages. Describe such a method briefly.

(3) Consider sending messages from sender A to receiver B in such a way that the messages sent from sender A cannot be eavesdropped on the network and receiver B can verify that the messages are not falsified. Describe what kind of methods should be applied at sender A and receiver B in order to implement this feature using a public key cryptographic technique.

(4) Describe what kinds of risks exist when sender A generates the ciphertext messages to receiver B, if a third-party X falsely gives the public key of X (K_p^X) as the public key of B to sender A. Also answer some ideas to avoid those risks.