張　一鳴

21B12111

課題6-1:

nを超えないために暗号化可能な平文の長さ512bitになります。

課題6-2:

(1)

であるので、e=5とおく。

1. 𝐾𝑅={𝑑,𝑛} = {77, 119}

(2)

暗号文

(3)

課題6-3:

横軸はと縦軸は対数です。は二つ同じ桁の素因数の乗算の結果で、縦軸はnを分解する時間の対数この図から見るとぐらいの素数の分解時間がやく1秒です。素因数分解の計算に1年以上を要する

素因数分解にかかる時間はnの大きさと直接に関係がなく、nの素因数の中で一番大きいファクター関係します。つまり、であるときに、分解時間がとなります。 言い換えると、最大な素因数が10倍になったら、素因数分解にかかる時間の10倍となります。q=1009の時、一回あたり処理時間が約sであるので、 の素数であるとき、一回あたり処理時間が1sくらいになると推定します。くらいの素数であるとき、素因数分解の計算に1年以上を要する。また、もう一つの素因数は、を満たす。つまり、くらいの値だと推測します。

課題6-4:

平文: Hi, there. This is a plaintext. My name is SSS.

*平文(HEX):*

*0x48 0x69 0x2C 0x20 0x74 0x68 0x65 0x72 0x65 0x2E 0x20 0x54 0x68 0x69 0x73 0x20 0x69 0x73 0x20 0x61 0x20 0x70 0x6C 0x61 0x69 0x6E 0x74 0x65 0x78 0x74 0x2E 0x20 0x4D 0x79 0x20 0x6E 0x61 0x6D 0x65 0x20 0x69 0x73 0x20 0x53 0x53 0x53 0x2E*

*暗号文(HEX):*

*0x67 0x0D 0xC8 0x31 0x08 0x4C 0x58 0x94 0x63 0x36 0xA2 0x6A 0xC5 0xAE 0x2D 0x40 0xCB 0x31 0xD3 0xC2 0xD7 0x57 0x71 0x22 0xAC 0x19 0x62 0xEC 0xFD 0xA1 0xAF 0xCE 0xD3 0xF8 0x03 0xD6 0x1D 0xE6 0x66 0x2E 0xC9 0x01 0xD3 0x4E 0xED 0x4B 0x8A 0x7E 0x9D 0x59 0xA0 0x8B 0xCA 0xD6 0xC6 0xA4 0x99 0x4A 0xE7 0x45 0x9C 0x10 0x79 0xDB*

*復号文: Hi, there. This is a plaintext. My name is SSS.*

*復号文(HEX):*

*0x00 0x02 0x6B 0xCD 0xD1 0x90 0x29 0x70 0x46 0xFE 0xDB 0x0C 0x76 0x33 0x33 0x43 0x00 0x48 0x69 0x2C 0x20 0x74 0x68 0x65 0x72 0x65 0x2E 0x20 0x54 0x68 0x69 0x73 0x20 0x69 0x73 0x20 0x61 0x20 0x70 0x6C 0x61 0x69 0x6E 0x74 0x65 0x78 0x74 0x2E 0x20 0x4D 0x79 0x20 0x6E 0x61 0x6D 0x65 0x20 0x69 0x73 0x20 0x53 0x53 0x53 0x2E*

課題6-5:

RSA暗号の鍵が512ビット(64バイト)であり、暗号化する時にパディング方式がRSA\_PKCS1\_PADDINGに指定されており、平文が164バイト未満である場合、ランダムなデータが平文の中にパディングされます。6-4の平文は512ビット(64バイト)未満なので、平文の中にランダムなデータが入り、同じ平文および鍵を用いて暗号化、復号を行った場合でも、実行するたびに、生成される暗号文、復号文は変化します。

課題6-6:

平文:

This is a message for the RSA digital signature.

SHA256 digest:

0xFF 0xAE 0x5A 0xF7 0x3C 0xA2 0x51 0xC4 0xE4 0x91 0xE6 0x84 0x61 0x6D 0xD3 0x3A 0x51 0x97 0x8A 0x9A 0x40 0x4A 0x04 0xB8 0xF7 0x50 0x83 0x38 0xC9 0x08 0x29 0x70

署名文:

0xAB 0xC2 0x9C 0x12 0x4A 0x5B 0x62 0xB5 0xD6 0x4E 0x3E 0x4A 0xC2 0xB9 0xA2 0x4F 0xA9 0x03 0xE2 0xE3 0x8D 0x94 0x51 0x34 0xC3 0xA5 0xB9 0x69 0xFF 0x84 0x6C 0x0C 0x3A 0x5D 0xF3 0x19 0x83 0x9C 0xB4 0x80 0x25 0x2C 0xE2 0x5D 0x33 0x4E 0xD5 0xE0 0x89 0xFE 0x2D 0x9F 0xF8 0xC7 0x6F 0x00 0x1F 0xE9 0xB4 0xCB 0xC0 0x74 0xC8 0x91

署名検証用データ(HEX):

0x30 0x31 0x30 0x0D 0x06 0x09 0x60 0x86 0x48 0x01 0x65 0x03 0x04 0x02 0x01 0x05 0x04 0x20 0xFF 0xAE 0x5A 0xF7 0x3C 0xA2 0x51 0xC4 0xE4 0x91 0xE6 0x84 0x61 0x6D 0xD3 0x3A 0x51 0x97 0x8A 0x9A 0x40 0x4A 0x04 0xB8 0xF7 0x50 0x83 0x38 0xC9 0x08 0x29 0x70

課題6-7:

メッセージをSHA-256でハッシュすれば、32バイトのメッセージダイジェストとなります。ハッシュ値が64バイト未満なのでランダムなデータに加えてRSA\_sign()、秘密鍵で暗号化する時、signatureが64バイトとなります。RSA\_public\_decryptした後の署名検証用データも64バイトです。そうなると、ハッシュ値と検証用データが一致しないにもかかわらず、署名検証成功することがあります。

課題6-8:

Problem1.txt.sig と　Problem4.txt.sigです。

課題6-9:

セキュリティ鍵長 80bit

RSA 1024bit 暗号化（100,000回）CPU使用時間：1.22 秒

RSA 1024bit 復号（100,000回）CPU使用時間：14.35 秒

2Key Triple-DES暗号化（100,000回）CPU使用時間：0.59 秒

2Key Triple-DES復号（100,000回）CPU使用時間：0.57 秒

セキュリティ鍵長 112bit

RSA 2048bit 暗号化（100,000回）CPU使用時間：3.64 秒

RSA 2048bit 復号（100,000回）CPU使用時間：73.59 秒

3Key Triple-DES暗号化（100,000回）CPU使用時間：1.13 秒

3Key Triple-DES復号（100,000回）CPU使用時間：1.10 秒

セキュリティ鍵長 128bit

RSA 3072bit 暗号化（100,000回）CPU使用時間：7.33 秒

RSA 3072bit 復号（100,000回）CPU使用時間：324.12 秒

AES暗号化（100,000回）CPU使用時間：0.05 秒

AES復号（100,000回）CPU使用時間：0.06 秒

RSA暗号の暗号化と復号にかかる時間は非対称性があります。その理由はRSAで使われるがより小さいと考えています。復号するときにべき乗演算の回数が暗号化するときに比べてずっと多いので、復号化処理にかかる時間が長いです。

課題6-10:

送った分について:

学生氏名: 楊　家寧

平文: Hello, yang. My name is zym. I want to send you this message. Thank you very much.暗号文:

学生氏名: 劉　仕奇

平文: Hello, yang. My name is zym. I want to send you this message. Thank you very much.暗号文:

学生氏名: 大山　雄右

平文: Hello,　I am an undergraduate student from Tokyo Tech.

暗号文:

0: 47 02 e8 bb 10 1a a1 56 82 9e b2 2e 76 79 fa 16 : G......V....vy..

16: c7 65 50 03 f1 7b b1 bf 87 0c fa 93 4f 1e 34 93 : .eP..{......O.4.

32: 1a ba d8 cd de 50 6d ec ee 83 07 88 3e 55 b2 24 : .....Pm.....>U.$

48: 01 69 e5 a9 60 4e ab 21 c5 f0 b3 d1 07 bc 84 9a : .i..`N.!........

もらった分について:

学生氏名: 楊　家寧

暗号文:

復号文:

学生氏名: 劉　仕奇

暗号文:

復号文:

学生氏名: 大山　雄右

暗号文:

0: 9c 16 1c 3f 1a 5d 2c fa 94 1c e9 b4 b4 f5 33 5b : ...?.],.......3[

16: 6c 1d e6 08 b2 eb 68 41 14 3b 4e 88 f0 00 bb 9c : l.....hA.;N.....

32: 00 c4 0c 04 9b 97 a0 18 e1 8d 15 44 55 24 37 c7 : ...........DU$7.

48: 0b 80 be 4e 39 a6 a7 6c 65 25 e7 6f ec 65 ea 61 : ...N9..le%.o.e.a

復号文:

I am Yusuke Oyama.

共通鍵暗号方式では事前に第三者に漏れないように鍵を受信者に共有する必要があります。

公開鍵暗号方式では公開鍵が第三者に知られても良いので、どんな方法で鍵を共有してもかまわないです。秘密鍵だけを安全に保管します。

と公開鍵暗号方式の鍵配送における違いを考察せよ。

課題6-11:

発行者: Tokyo Tech Portal CA G2

有効期限の終了日: ‎2025‎年‎4‎月‎15‎日 23:59:59

Comman Name: C0676705