DM534 — Øvelser Uge ??

Introduktion til Datalogi, Efterår 2021

Jonas Vistrup

1 I

1.1

Suppose a public RSA key is $PK = (1517, 13)$. Which of the following is the RSA encryption of the message 43?

(a) $1517^{43} \pmod{13}$

(b) $43^{13} \pmod{1517}$

(c) $13^{43} \pmod{1517}$

SVAR: b

1.2

Is one of the following the multiplicative inverse of 49 modulo 221? Or does no multiplicative inverse exist?

$$12, 56, 121, 212$$

SVAR: 212 is the multiplicative inverse of 49 modulo 221.

1.3

Which of the following is a valid RSA key (ignoring the fact that the numbers are not large enough for security)?

(a) $PK = (91, 37); SK = (91, 23)$. **SVAR:** Invalid. $37 \cdot 23 \mod 12 \cdot 6 = 59$.

(b) $PK = (143, 77); SK = (143, 53)$. **SVAR:** Valid.

(c) $PK = (231, 59); SK = (231, 47)$. **SVAR:** Invalid. $231 = 3 \cdot 7 \cdot 11$.

(d) $PK = (107, 25); SK = (107, 30)$. **SVAR:** Invalid. 107 is prime.

1.4

In the Sieve of Eratosthenes (page 54 on the slides), how many lists (including the current) have been created at the point where the number 13 is the first element in a list?

SVAR: 6, since 13 is the sixth prime.

1.5

Consider an RSA system with Alice's public key $N = 1517$ and $e = 17$. Note that $1517 = 37 \cdot 41$.

(a) Find Alice's secret key d. Use the Extended Euclidean Algorithm from pages 47–48 of the RSA slides used in lectures (there, e and d are called a and s (and d also is called x at top of page 48)).

(b) Try encrypting 423. Use the algorithm for fast modular exponentiation (page 30 on the slides). How many times during the recursive execution is the "if k is odd" case encountered, and how many times is the "if k is even" case encountered? [Do not include the base cases k = 0 and k = 1 in the counts.]

(c) Decrypt the number obtained above, using fast modular exponentiation. Is the result correct? How many times during the recursive execution is the "if k is odd" case encountered, and how many times is the "if k is even" case encountered? [Do not include the base cases k = 0 and k = 1 in the counts.]

SVAR a: $d = 593$.

SVAR b:

$$\begin{aligned}
423^{17} \mod 1517 = 423 \cdot z \mod 1517 & \\
z &= 423^{16} \mod 1517 = c_1 \cdot c_1 \mod 1517 \\
c_1 &= 423^{8} \mod 1517 = c_2 \cdot c_2 \mod 1517 \\
c_2 &= 423^{4} \mod 1517 = c_3 \cdot c_3 \mod 1517 \\
c_3 &= 423^{2} \mod 1517 = c_4 \cdot c_4 \mod 1517 \\
c_4 &= 423^{1} \mod 1517 = 423 \\
c_3 &= c_4 \cdot c_4 \mod 1517 = 423 \cdot 423 \mod 1517 = 33 \\
c_2 &= c_3 \cdot c_3 \mod 1517 = 33 \cdot 33 \mod 1517 = 1089 \\
c_1 &= c_2 \cdot c_2 \mod 1517 = 1089 \cdot 1089 \mod 1517 = 1144 \\
z &= c_1 \cdot c_1 \mod 1517 = 1144 \cdot 1144 \mod 1517 = 1082 \\
423^{17} \mod 1517 = 423 \cdot z \mod 1517 &= 423 \cdot 1082 \mod 1517 = 1069
\end{aligned}$$

1 odd, 4 even.

1.6

Why is a cryptographically secure hash function used in connection with RSA digital signatures?

SVAR: Hash function, for size reduction. Cryptographically secure, so it's improbable to change the message without changing the hash.

1.7

With RSA, why would you never use the value 2 as one of of the two primes p and q?

SVAR: Because it would result in a even N_a ensuring that everyone knows that you used 2. From there the second prime is easily found.

1.8

In RSA, why must the message being encrypted be a non-negative integer strictly less than the modulus?

SVAR: Modulus returns the non-negative remainder between 0 and the modulus-1. If larger numbers (or negative numbers) are used then multiple messages would encrypt to the same number, and the decrypted cipher would not lead to the orignal message.

2 II

2.1

Try breaking these two encrypted messages:

(a) This English message was encrypted using a Caesar cipher. Decrypt it.

YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

Discuss which techniques you used. [Hint: You may want to write a simple program to help you try out things.]

SVAR: SHIFT A->V: THIS CRYPTOGRAM IS EASY TO DECIPHER.

(b) This was entitled ”Cold Country”. It was encrypted using a monoalphabetic substitution cipher. A monoalphabetic substitution cipher works similarly to a Caesar cipher. However, instead of just shifting the alphabet cyclically by a fixed amount to get the mapping defined for each letter, the alphabet is permuted (reordered) arbitrarily. In other words, in such a cipher the key is a permutation of the alphabet which tells what letter “A” maps to, what letter “B” maps to, etc. If the alphabet has 29 letters, the number of keys is now 29! Why? (**A key for each possible combinations.**) The original message here was in English, so there are only 26 letters. How many possible keys are there? (**26!**)

TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC. UFYR FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB BWWR CWWD.

Discuss which techniques you used. [Hint: Use knowledge (or good guesses) of frequencies of letters in English. You may want to write a simple program to help you try out things.]

SVAR:

’A’,’F’,’D’,’P’,’W’,’O’,’G’,’A’,’V’,’N’,’K’,’P’,’U’,’N’,’R’,’L’,’C’,’T’,’W’,’G’,’M’,’V’,’E’,’H’,’S’,’I’