Institut for Matematik og Datalogi
Syddansk Universitet, Odense

3. december 2020
JFB/RF

Opgaver DM534 uge 49/50

Husk at læse de relevante sider i slides og noter før du/I forsøger at løse en opgave.

I: Løses i løbet af øvelsestimerne i uge 49

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

   For the correct answer among those above, we want to use the algorithm for fast modular exponentiation (page 30 on the slides) to calculate the encrypted message. 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.]

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

   12, 56, 121, 212

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

   (a) $PK = (91, 37)$; $SK = (91, 23)$
   (b) $PK = (143, 77)$; $SK = (143, 53)$

   (c) $PK = (231, 59)$; $SK = (231, 47)$
   (d) $PK = (107, 25)$; $SK = (107, 30)$

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?

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.]

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

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

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

II: Løses hjemme inden øvelsestimerne i uge 50

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.]

(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 (re-ordered) 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? The original message here was in English, so there are only 26 letters. How many possible keys are there?

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.]