Problem sheet 4
2018

Codierungstheorie und Kryptographie

20. Decipher the following text, (the plain text is english.) It's a world famous cryptogram.

    53 ‡ ‡ † 305))6∗; 4826)4 ‡ .)4‡); 806∗; 48 † 8
    ¶60))85; ;]8∗; : ‡ ∗ 8 † 83(88)5∗; 46(; 88 ∗ 96
    ∗?; 8) ∗ ‡(; 485); 5 ∗ †2 : ∗ ‡ (; 4956 ∗ 2(5 ∗ 4)8
    ¶8∗; 4069285);)6 † 8)4 ‡ ‡; 1(‡9; 48081; 8 : 8 ‡
    1; 48 † 85; 4)485 † 528806 ∗ 81(‡9; 48; (88; 4
    (‡?34; 48)4‡; 161; : 188; ‡?;

21. Bob chooses $p = 101, q = 113$. Compute $n, \varphi(n)$. Bob chooses $b = 3533$. Test if b is admissable. Compute (in detail) $b^{-1} \mod n$ and a.
    Alice wants to send the message 9726. How does she encrypt, and how does Bob decrypt?

    Apply the square and multiply algorithm for large powers.

22. a) RSA is insecure, if one can factor $n = pq$. If the primes p and q are very close, then one can factor n with a few attempts. Write $n = 56759$ as a difference of two squares $n = s^2 - t^2$ and use this to factor n.

    b) Now analyze the situation more generally and prove that $q < p \leq (1 + \varepsilon)\sqrt{n}$ implies that one has to test at most $\frac{\varepsilon^2}{2}\sqrt{n}$ many values s. Assuming that $n = 10^{100}$ and that one can do 10^{20} tests. Give a lower on the difference $p - q$.

23. The following algorithms factors an integer $n = pn'$, if $p - 1$ consists of small prime power factors $q \leq B$ only.
    $a_1 = 2$
    { for $j = 2$ to B
    $a_j = a_{j-1}^j \mod n$
    }
    $d = \gcd(a_B - 1, n)$.
    If $1 < d < n$, then d is a divisor of n.

    Prove that the algorithms finds a divisor, if all prime power factors of $p-1$ are $q \leq B$.
    Hints $(p - 1) \mid B!$, and choose $a \equiv 2^{B!} \mod n$.

    Now let $n = 15770708441$ and $B = 180$, compute a and hence find a divisor.

    Note: 1) as $B!$ is quite large, one does not really compute $2^{B!}$, but rather $2^{B!} \mod n$. You can always keep the numbers small.
    2) Also, you are not supposed to compute $\varphi(n)$, as this would require factoring.

24. In this exercise we show that RSA is not secure against a chosen cipher text attack. Given a cipher text y, choose another cipher text y', such that your knowledge yof $x' = d_K(y')$ allows to compute $x = d_K(y)$. (Hint compare $e_K(x_1)e_K(x_2) \bmod n$ and $e_K(x_1x_2 \bmod n)$.)

25. Factor $n = 256961$ using the random squares algorithm, with factor base $\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$. Test the integers $z \geq 500$ until you find $x^2 \equiv y^2 \bmod n$, and find the factorization.