Problem sheet 5
2020

**Codierungstheorie und Kryptographie**

33. 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; ‡?;

34. For RSA: 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.

35. 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 bound on the difference $p - q$.

36. 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.

37. 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 of $x' = d_K(y')$ allows to compute $x = d_K(y)$. (Hint: compare $e_K(x_1)e_K(x_2) \bmod n$ and $e_K(x_1x_2 \bmod n)$.)

38. 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.

39. (a) (Probably you did this one in a probability course): Let $S$ be a set of $q$ persons, randomly chosen from a large set of persons whose birthdays are uniformly independently distributed (u.i.d.) over the 365 days of a year. Determine the minimum number $q$ such that the probability that there are at least two persons (among the $q$) having the same date as their birthday exceeds $p_1 = \frac{1}{2}$ or $p_2 = 0.999$. How does $q$ change, if the concept of birthday is appropriately generalized, so that all persons have a u.i.d. label $b \in \{1, \ldots, N\}$, determine $q$ as a function of $N$ and $p$.

    (b) Fix $x \in \mathbb{Z}_N$, and randomly (u.i.d.) choose $r_1, \cdots, r_q \in \mathbb{Z}_N$. Show, when $q = \lfloor \sqrt{2N} \rfloor$ the probability that there exist $i$ and $j$ such that $r_i = x + r_j \bmod N$ is at least $p = 0.6$.

    (c) Let $p$ be a prime, and let $g \in \mathbb{Z}_p^*$ be a primitive root. Show that one can find in $\mathbb{Z}_p^*$ the discrete logarithm of $X$ to base $g$, if one can find $r$ and $s$ with $g^r = Xg^s \bmod p$. Use this and part b) to describe an algorithm which solves in $O(\sqrt{P})$ steps the discrete logarithm problem, with high probability.

40. Read about "birthday paradox attack". Apply it to signature schemes, where you want to persuade Alice to sign a document $m$, which she refuses to sign.

    Hint: create many essentially identical versions of $m$, (but with tiny changes, such as extra spaces), and also a quite different document $M$ with many essentially identical versions that Alice would agree to sign.

    How does the underlying idea of the birthday paradox help you to forge Alice's signature on your preferred document $m$ (or any of its versions)?

41. If the message $m$ is long, (say a book of 500 pages!), and one performs any operation such as $m^a \bmod n$, then this is a quite long=expensive computation. Suggest how one can keep high security but reduce the costs. (There may be plenty of ideas, but also read about hash functions.)