Homework 9 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

17.01.2014

Exercise 24.
Let $x, y \in \mathbb{Z}, a \in \mathbb{Z}_n^\star \setminus \{1\}$, and $\operatorname{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \pmod{n}\}$.

(a) Show that $a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{\operatorname{ord}_n(a)}$.

Exercise 25. Prove Proposition 7.5 from the lecture, which provides a possibility to check whether a is a primitve element modulo n:

Let $p > 3$ be prime and $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$.
Then, $a \in \mathbb{Z}_p^*$ is a primitive element modulo $p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}$ for all $i \in \{1, \dots, k\}$.

Exercise 26. Alice and Bob are using Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31337$ for their communication. Alice chooses the random number $a = 9999$ while Bob chooses $b = 1011$. Alice's message is $m = 3567$.

(a) Calculate all exchanged values c_1, c_2, and c_3 following the protocol.
Hint: You may use $6399^{1011} \equiv 29872 \pmod{31337}$.

Exercise 27. Consider the following insecure cryptosystem:
Alice secretly chooses four integers $a, b, a', b' \in \mathbb{N}$, with $a > 1, b > 1$, and computes

$$M = ab - 1, \qquad e = a'M + a, \qquad d = b'M + b, \qquad n = \frac{ed - 1}{M}.$$

Her public key is (n, e), her private key is d. To encrypt a plaintext m, Bob uses the map $c = em \bmod n$. Alice decrypts the ciphertext received from Bob by $m = cd \bmod n$.

a) Verify that the decryption operation recovers the plaintext.

b) How can the Euclidean algorithm be applied to break the cryptosystem.