Homework 10 in Advanced Methods of Cryptography

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

18.12.2012

Exercise 29. Consider the following public-key cryptosystem:

Alice chooses four integers a, b, a' and b'. She caluclates the values:

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

Her public key is (n, e) and her private key is d. A plaintext m is encrypted by $c \equiv em \, (mod \, n)$. Alice deciphers c by computing $cd \equiv m \pmod{n}$.

(a) Verify that the decryption operation recovers the plaintext.

(b) Break the system by means of the Euclidean algorithm.

Exercise 30.

Consider an RSA cryptosystem with $n = pq$ with two primes $p \neq q$ and a public key $e = d^{-1} \pmod{\varphi(n)}$. The plaintext m is in the set $\{1, \ldots, n-1\}$.

(a) Show that it is possible to compute the secret key d if m and n are not coprime, i.e. if $p \mid m$ or $q \mid m$.

(b) Calculate the probability for m and n having common divisors.

(c) How large is the probability if n has 1024 bits? The primes p and q are approximately of same size $(p, q \approx \sqrt{n})$.

Exercise 31.

Alice is using the ElGamal cryptosystem for encrypting the messages m_1 and m_2.

The generated cryptograms are

$$\mathbf{c}_1 = (1537, 2192) \text{ and } \mathbf{c}_2 = (1537, 1393).$$

The public key of Alice is $(p, a, y) = (3571, 2, 2905)$.

(a) What has Alice done wrong here?

(b) The first message is given as $m_1 = 567$. Determine the message m_2.