COMPUTER NETWORKS

EXERCISES LIST 5

1. Assume we encrypt to messages a and b with the same key k using *one-time pad* method (the length of message and key are equal). In result we obtain two ciphertexts a' and b'. Show that if an attacker has both ciphertexts (i.e. a' and b') and obtains one of the original messages (i.e. a), he can decode the other original message (i.e. b).

2. Choose two prime numbers p and q such that $p > q > 5$ holds. Generate pair of RSA keys – private and public. Encrypt message `10010100111010100010` with your public key, and then decrypt it with your private key.

3. Extend proof of RSA correctness for any $m \in [0, n]$. The proof is provided in the handouts.

4. Let $n = p * q$, where p and q are prime numbers. Show that if one knows $\phi(n)$ he can factorize n in polynomial time.

5. Let every third e-mail to be a spam message. Word `enlarge` occurs in 80% of spam e-mails and in 5% of non-spam e-mails. We fetched an e-mail with `enlarge` word in it – what are the chances[1], that it's a spam?

6. A deterministic hash function h is given, that for a text message returns m-bit number. We choose $2^{m/2}$ random text messages and for them we calculate value of h function. Let's assume that with such selection of x text message, $h(x)$ is randomly (with uniform distribution) chosen m-bit number. Show that within the set of text messages described above there are two text with the same value of hash function h with probability of $\Omega(1)$.

Marcin Bieńkowski
Translation: *Krystian Bacławski*

[1] Using word "probability" wouldn't be mathematically correct here, because the e-mail is not chosen from pool of all messages.