T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 9 – Solutions
Tue 8.4.2003 12–14 T3 and Wed 9.4.2003 18–20 T1

1. **Are there any truly provably secure encryption methods ?**

   Yes there is. We may simply use one-time-pads. In fact, from the view-point of Shannon's information theory, a necessary requirement for *perfect secrecy* is that the secret is key is of equivalent length (in entropy bits) to the message.

   Where "cost" is not a problem, such as for spies and diplomats, OTPs are widely used.

2. **What is the main difference between a "one-way function" such as the RSA problem and a "one-way function" such as SHA-1 ?**

   The former falls into the conjectured class of *trapdoor one-way functions*. That means that the inverse of SHA-1 is thought to be hard to compute in all cases; there is no shortcut for computing the inverse except than to actually know it.

   O.t.o.h. if $\phi(n)$ or the factorization of n is known, the RSA trapdoor $C = M^e \mod n$ is easy to invert.

3. **Discuss the security assumptions of each one of the following cryptographic algorithms:**

   - **RSA Signature Algorithm (say - PKCS #1 v2.1)**

     In this particular case we are assuming that a) the message digest (hash) function is one-way and b) RSA problem is hard. Furthermore, we are assuming that factorization is hard, $P \neq NP$ etc.

   - **Naor-Reingold Number-Theoretic PRF**

     The only assumption is that decisional Diffie-Hellman is hard. This also implies that discrete logarithm problem is hard in the given group.

   - **Advanced Encryption Standard.**

     The security is based almost entirely upon purely heuristic basis. We only know that no-one has reported finding an attack against AES that is faster than exhaustive key search.

   - **A "provably secure" mode of operation for AES.**

     The basic assumption is that AES is hard to distinguish from a PRP. Otherwise the proof should be watertight.

   - **Secure Socket Layer 3.0**

     The proof is purely heuristic. All component parts (e.g. encryption, message authentication, key exchange, signature, communication protocol design) are assumed to be secure on heuristic basis. Some proofs of protocol correctness under certain model does exist now, though.

4. **Mount a known-plaintext (distinguishing) attack against CBC mode with random IV's. What is the appropriate oracle model ? How would you use the birthday paradox in this case ?**

   The correct model is to try to distinguish between a random permutation and the output from CBC encryption. [picture]

   We have a sequence of encrypted messages and the corresponding plaintext. Each message contains the (random) IV as the first block. We will not care about such things as the correlation of the message lengths, padding etc.

   By birthday paradox we may expect the encryption to function to get the same input block after about $2^{l/2}$ blocks. Since the corresponding plaintexts also match, distinguishing is possible.

   It is noteworthy that this simple attack comes very close to the provable security bound of CBC encryption.