Cryptography and Networked Systems Security

Prof. Dr.-Ing. Volker Roth
Freie Universität Berlin

Homework 4

Academic Integrity

Hereby I certify that I have neither received nor given help in answering the questions in this homework assignment.

_____

Date, signature, name in block letters

Question 1 (10 pts.)

Say $\Pi = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$ is a secure MAC, and for $k \in \{0,1\}^n$ the tag-generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that t must be super-logarithmic.
Hint: Show $t(n) = \mathcal{O}(\log n) \Rightarrow \Pi$ is no secure MAC.

Question 2 (10 pts.)

Let (Gen, H) be a collision-resistant hash function. Is $(\mathrm{Gen}, \bar{H})$ with $\bar{H}^s(x) := H^s(H^s(x))$ necessarily collision resistant?

Question 3 (10 pts.)

Consider a modified substitution-permutation network where the cipher instead first applies r rounds of key-mixing, then carries out r rounds of substitution, and finally applies r permutations. Analyze the security of this construction.

Question 4 (10 pts.)

DES has the so-called complementarity property. This means that

$$\mathrm{DES}_k(x) = \overline{\mathrm{DES}_{\overline{k}}(\overline{x})}$$

for $k \in \mathcal{K}$ and $x \in \mathcal{M}$. Construct an algorithm, which finds the key of DES in time 2^{55} with probability 1.
Hint: Use a chosen-plaintext attack with two carefully chosen plaintexts.

Question 5 (5 pts.)

Let $N = pq$ the product of two distinct primes. Give an polynomial algorithm which takes as input N and $\varphi(N)$ and computes p and q.

Question 6 (5 pts.)

How many Operations are needed to encrypt a message with $e = 2^{16} + 1$ in RSA?

Question 7 (5 pts.)

Alice sends $c = 468$ to Bob, who uses the RSA-key $(n, e) = (899, 11)$. Find m!

Question 8 (10 pts.)

[Common-Modulus Attack]

You received two encrypted ciphertexts $c_e \equiv m^e \mod n$ and $c_f \equiv m^f \mod n$, which were made by encrypting the same messages twice with two different RSA keys (e, n) and (f, n). Show that if $\gcd(e, f) = 1$ you can easily calculate m.