Homework 6 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

14.06.2007

Exercise 15.
Generate DSA-parameters of a size which is reasonable for cryptographic applications.

Exercise 16
Let G be a finite Abelian group and $g_1, g_2 \in G$. Let e_1 and e_2 be positive integers. Describe a "square-and-multiply"-like algorithm for the efficient computation of $g = g_1^{e_1} g_2^{e_2}$. This algorithm should not compute g by multiplying $g_1^{e_1}$ and $g_2^{e_2}$.

Hint: Use a table of precomputed values $g_{b_1,b_2} = g_1^{b_1} g_2^{b_2}$, $b_1, b_2 \in \{0, 1\}$.

Exercise 17.
Construct a Challenge-Response-Protocol allowing Alice and Bob to authenticate each other. The protocol should be based on public key cryptography. Is it possible to construct such a protocol without a hash function and only 3 rounds of communication?

Exercise 18.
You somehow retrieved the following snippet from an /etc/shadow file:

```
bruce:Ff7bmZdi4XkW2:13390:0:99999:7:::
peter:/XiNtks7k/6jw:13390:0:99999:7:::
michael:QE0LTn.KNh2C6:13390:0:99999:7:::
noob:QurvKbvvjbR7g:13390:0:99999:7:::
mathar:Q9fzIw/ypqRLI:13390:0:99999:7:::
```

Crack the passwords.

The file is also available for download on the lecture homepage.