



# CRACKING SHA1-HASHED PASSWORDS

Author: Chair for Cryptology and IT-Security

March 2011

# SHA1

The *Secure Hash Algorithmus 1* has been standardized by the National Institute of Standards and Technology in 1995 and is besides MD5 the most commonly used hash algorithm in practice. An example for its usage is password-based authentication. In that case, the server does not store the user password in plain text but instead the SHA1 hash value of it. Once the user enters his password and after its received at the server, its hash value is computed and compared to the value stored on the server in order to verify its correctness.

# Scenario

A vulnerability of a surveillance system's webserver leaked the SHA1 hash value of the password of the administrator account. The password's hash value is

67ae1a64661ac8b4494666f58c4822408dd0a3e4

Furthermore, the keyboard of the login terminal shows clear signs of the entered password since after a successful login navigation in the software is only done via arrow keys.

What is the password?



**Figure:** Fingerprints on the keyboard

*Remark: Note the German keyboard layout!*