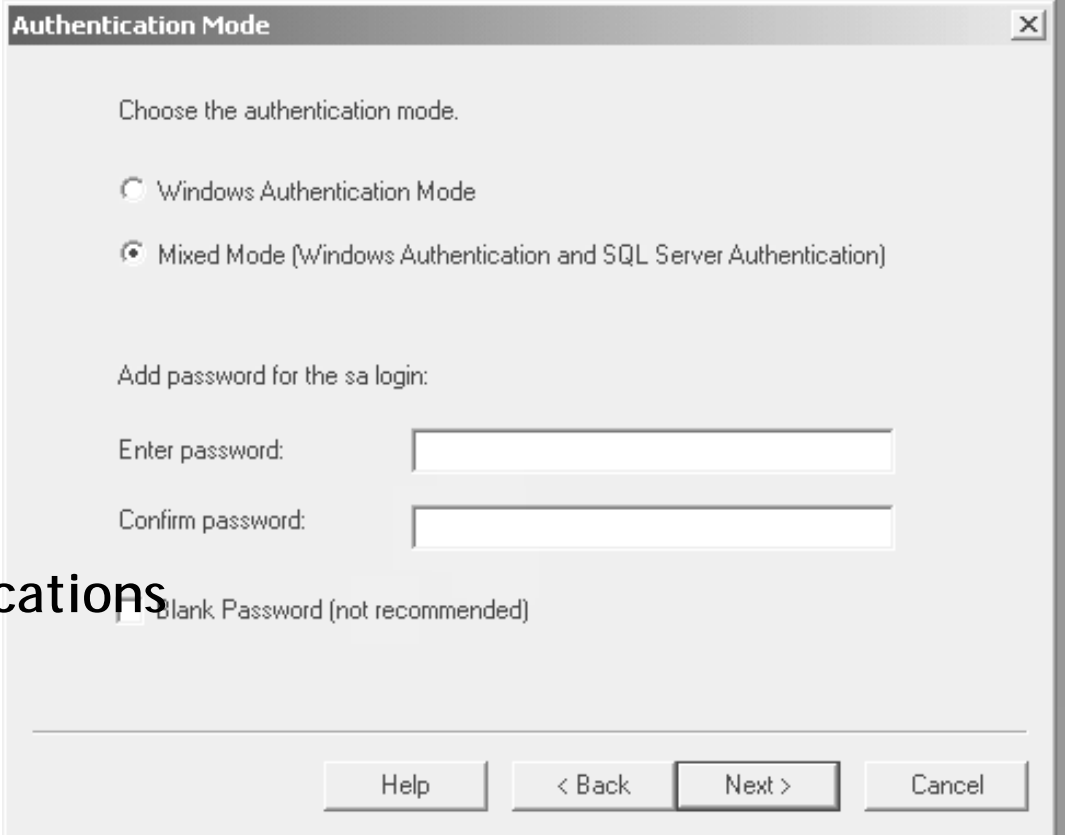


# Assignment 3: Cryptography

Information and Communications  
Security (SS 2008)

Prof. Dr. Kai Rannenberg

T-Mobile Chair for  
Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.  
[www.whatismobile.de](http://www.whatismobile.de)



Authentication Mode

Choose the authentication mode.

Windows Authentication Mode

Mixed Mode (Windows Authentication and SQL Server Authentication)

Add password for the sa login:

Enter password:

Confirm password:

Blank Password (not recommended)

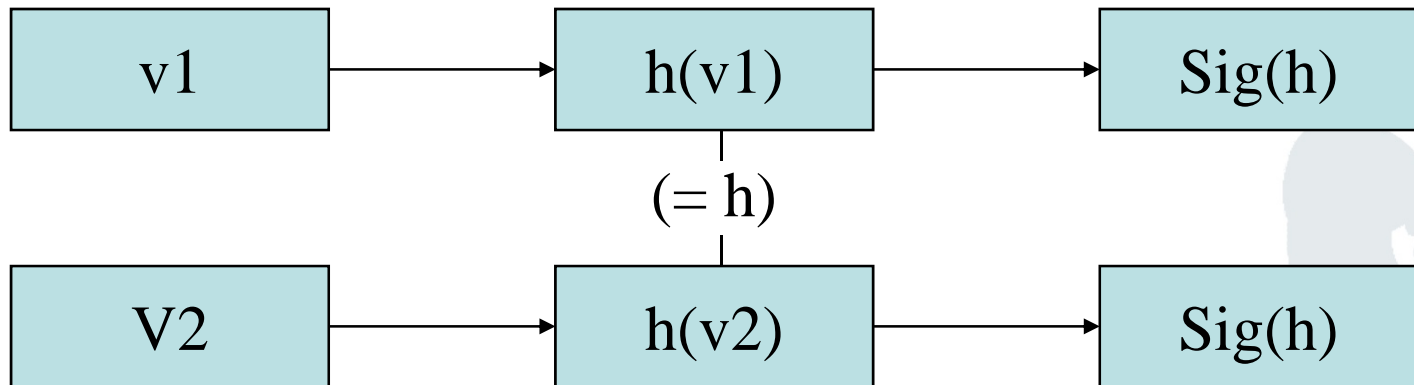
Help < Back Next > Cancel

- Install GnuPG or a similar software for mail encryption on your system. Create a new key pair, and send a signed and encrypted message to [sec@m-chair.net](mailto:sec@m-chair.net) containing your newly created public key and a short summary of your experiences.
  - Practical exercise, no solution here, check script for overview of PGP
  - Be careful to only send your public key
  - You can also send your existing public key, but in this case be extra careful NOT TO SEND US YOUR PRIVATE KEY, thank you.
  - If you haven't done this yet, try it, sending encrypted mail is useful, and we want you to be able to do it.

- Scenario: A cryptographer has published an algorithm that allows him to find pairs of values  $v_1, v_2$  such that  $h(v_1)=h(v_2)$ , for a hash function  $h$ .
  - Which security properties of the function has he broken, which are not directly affected?
  - Describe an attack on a signature system using  $h$  resulting from the attack on the hash function ( $h$ ).

- Which security properties of the function has he broken, which are not directly affected?
  - (Strong) collision resistance broken
  - However, one-way property not directly affected
  - Also, if one of the values  $v$  cannot be chosen freely by attacker, attack might still fail

- Describe an attack on a signature system using  $h$  resulting from the attack on the hash function ( $h$ ).
- $h(v1)=h(v2) := h$



- If message  $v1$  is signed, it may be exchanged for  $v2$

- Decrypt the following word, encrypted with the Caesar cipher:

UGEWTKVA

- Caesar: transposition, Caesar used  
A->C
- A->C works here
- Or try out A->B, A->C (only 26 possible keys [of which A->A doesn't make sense, but is valid])
- You may also use letter frequency tables, but not in this case (each letter appears 1 time only)

- UGEWTKVA (A->A)
  - A->B: TFDVSJUZ
  - A->C: SECURITY
  - A->D...
- „Security“ sounds good

- a) Describe differences between symmetric and asymmetric cryptosystems.
- b) Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.
- c) Describe different approaches towards the certification of keys.

- Describe differences between symmetric and asymmetric cryptosystems.
  - Asymmetric cryptosystems
    - Two keys: public and private
    - Key management by publication/certification of public keys
    - Relatively slow performance
  - Symmetric cryptosystems
    - One key: has to be kept secret from outsiders
    - Key management: sharing of keys via secure channels
    - Fast performance (-> For encryption of e.g. large files -> hybrid systems)

- Why is certification of public keys necessary? Name an attack that is possible if keys are not certified.
  - Makes sure acquired key really originates from correct entity.
  - Man-in-the-Middle-Attack: Exchange published public key (e.g. on server) for own. Decrypt, read, reencrypt passing messages

- Describe different approaches towards the certification of keys.
  - Certification hierarchy: Root certification authority which certifies keys of CAs one level below, which in turn certify keys of lower level CAs, users or other entities
  - Web of trust: Homogenous entities certifying each other's keys, degree of confidence in certification depends on trust in signing parties