Send secret msg

[Boxed and key]

by exchanging (Alice sends symmetric key)

RSA - asymmetric key/puible key encryption
Key

Adele Grade

Sign the form → Enc by

dec enam → gener lymph

Dust feed incubator (by Alice)
- MAN REPUDIABLE

- IM AGGRADABLE

- Cannot be lifted

- Can forget

- Must remember

Digit 1st grade
A hash, every password
  
  digest is built into the password.

- For a goal: a set of steps
  - The password is hashed and the hash is checked.
[Case]
Cut a Cheese... [case]

Obliques Transfer

Blink Syndrome

Free Statement

Corrections

Secure Communication

Authentication
A function

- Name, password
- What you know
- What you have
- What you can do

Authentication
proposed as for if time, key

challenge to time

{key, challenge}

host

client

key

user input

change

change

secret → password
- Password store can be stolen

- How to ensure passwords are not compromised when stored passwords are stolen

- Store password hashes.
old username

salt added here

<table>
<thead>
<tr>
<th>key = password</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
</tr>
<tr>
<td>25</td>
</tr>
<tr>
<td>text ( \rightarrow ) input</td>
</tr>
</tbody>
</table>

**SHA-1**

Salt.

**SHA-256**

2 characters saved.

Encrypt password to hash by 2 SHA-256.
- Check existence of password file
- Create backup of a set of data
- Discontinue old code