6.033 Lecture 23
Public-key Authentication

Nickolai Zeldovich

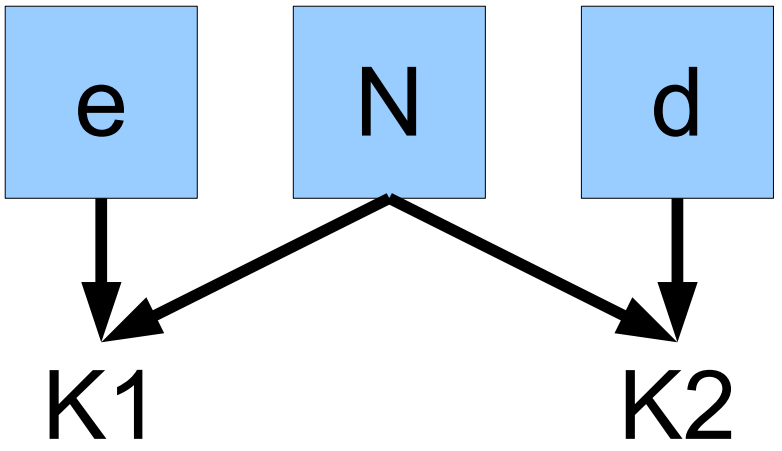
Spring 2009

RSA

Encrypt(m, {N, e}): $m^e \bmod N \rightarrow c$

Decrypt(c, {N, d}): $c^d \bmod N \rightarrow m$

Special property: $m^{ed} \bmod N = m$



Fraudulent Microsoft certificates

- In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation". The ability to sign executable content using keys that purport to belong to Microsoft would clearly be advantageous to an attacker who wished to convince users to allow the content to run. The certificates could be used to sign programs, ActiveX controls, Office macros, and other executable content.

...

Fraudulent Microsoft certificates

- ...

  VeriSign has revoked the certificates, and they are listed in VeriSign's current Certificate Revocation List (CRL). However, because VeriSign's code-signing certificates do not specify a CRL Distribution Point (CDP), it is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL.