Saving a Key

- We can read and write the bytes of a key to a file.
  - This is a bad idea.
- We want to
  - protect read access to private keys,
  - and make sure the publics ones are real.

KeyStores and Java keytool

- KeyStore provides password protected storage for keys.
- Most Java programs use existing keys rather than create keys themselves.
- The keytool command can be used to generate keys outside Java.

The KeyStore Class

- A KeyStore holds password protected private keys and public keys as certificates.
- Make keystores using the keytool e.g.

```
keytool -genkey -keyalg RSA
        -keypass password  -alias mykey
        -storepass storepass
        -keystore myKeyStore
```

Java demonstration

Pretty Good Privacy

- In 1991 Phil Zimmermann implemented RSA in an e-mail friendly package.
- He wanted encryption for everyone, especially activists.
- RSA inc. started a licensing dispute.
- The US government started a criminal investigation for arms trafficking!

The Crypto Wars

- Laws in the 1990s were unable to cope with strong encryption from short computer programs.
- Strong crypto available for free on the new Internet panic governments.
- Encryption algorithms and machines were classified as "arms" if key $>$ 40 bits.
- Who was going to control crypto in the age of the Internet?

The Crypto Wars

- 1991: proposed law in the US to ban public key crypto
- In reaction activists uploaded PGP on to Internet bulleting boards.
- 1993 arms trafficking case against Zimmermann started.
- 1993-1996 Investigation continues,
- people print RSA algorithm on t-shirts and go through U.S. customs
- PGP code printed as a book (freedom of speech).
- 1996 Case against Zimmerman dropped
- But U.S. Attorney: "no change in law, no change in policy"

The Crypto Wars

- 1993-1996: Clipper chip considered in US congress and rejected.
- Due partly to Matt Blaze's analysis and strongly attack by John Kerry among others.
- 2000 US laws lifted: the Geeks "won the crypto wars".
- Freedoms won in the US then filtered through to the rest of the Internet,
  - e.g. French laws until 2004: ECB mode only, max key length 40, must include known plain text.

Crypto Wars: Round 2

- We learnt in 2013 that the NSA had been working to weaken ("back door") crypto.
- Some of the possible backdoors:
  - "Bad" elliptic curve parameters
  - Weak random number generators: e.g. Dual_EC_DRBG

Crypto Wars: Round 2

- Manufacturers added smartphone encryption and end-to-end encryption for apps
- Governments don't like this: want the equivalent of wiretaps or access to decryption keys for police investigations
- Big problem: weakens crypto or introduces backdoors

Summary

- Public Key Cryptography uses one key for encryption (public key), another key for decryption (private key)
- Can make encryption key public, must keep decryption key secret
- Defined also key exchange algorithms (DH) which make it possible for participants to agree on a new key without anyone else knowing the key
- Defined public key algorithms RSA and ElGamal
- Public key cryptography can be used for signing: sign with private key and verify signature with public key