Cryptography and Security

2006 – 2007

Survey n° 7

Family Name: First Name:

Important Note:

Remember that there is only *one* correct answer to each question and that each *incorrect* answer looses you some points. It is preferable not to answer than to answer at random!

1. From a cryptographer's point of view, find the odd one out (*trouvez l'intrus*):

   ☒ FOX ☐ DES ☒ RSA ☐ IDEA

2. Diffie-Hellman is the name of a famous:

   ☐ MAC ☐ encryption scheme
   ☒ key exchange ☐ signature scheme

3. Tick the *correct* assertion. When doing hybrid encryption...

   ☐ ...the message is sent in clear.
   ☐ ...the message is encrypted with the public key of the recipient.
   ☐ ...the key used to encrypt the message is chosen by the recipient.
   ☒ ...the public key of the sender is not used at all.

4. Which of these is *not* included in an X.509 certificate:

   ☒ private key ☐ certificate signature
   ☐ identity ☐ expiry date

5. Tick the *true* assertion:

+

- ☐ PGP needs X.509 certificates.
- ☐ S/Mime doesn't need certificates.
- ☐ PGP requires a trusted CA.
- ☒ S/Mime is based on chains of trust.

6. On a Linux workstation, which of the following is stored on the disk but is not visible by standard (non-priviledged) users:

+

- ☒ password hashes
- ☐ username hashes
- ☐ passwords
- ☐ usernames

7. Thanks to the salt...

+

- ☐ ...different password never have the same hash.
- ☒ ...the same password can have different hashes.
- ☐ ...a password like "12345" is hard to guess.
- ☐ ...password hashes can be public.

8. When hashing a password on UNIX, using the DES-based technique. The password is...

+

- ☐ ...XORed to the hash.
- ☐ ...encrypted 25 times using the salt as a DES key.
- ☐ ...the hash of the salt.
- ☒ ...used as a DES key.

9. On a Pentium 4 computer, cracking passwords composed only of lower case letters of length 6 or less (using exhaustive search) takes in the order of:

+

- ☒ a minute
- ☐ an hour
- ☐ a day
- ☐ a year

10. Which of these names denotes a password cracking tool:

+

- ☐ Pot of Gold
- ☐ Adam
- ☒ Ophcrack
- ☐ Philip the Slayer

Fame is worthless.
G. Guninski