# Hands-on 7: Crypto

Michael Plasmeier

## Part 1

1. About $12$ days
2. About $1\*10^{25}$ years
3. About $7\*10^{14}$ lives of the Universe
4. It would still take about $1\*10^{7}$ billion years.
5. Around 82 to 83 years $\sum\_{i=0}^{}2^{i}\*1,000,000\*60\*60\*24\*365\*1.5$
6. Is it since 128 bits would take too long to crack anyway that additional bits don’t buy extra security?

## Part 2

1. c29518134a6b47563b1e411b7401a52c081996a4
2. Every user that calculates the SHA1 of this string will have the same result. I suppose you are asking for the chance any other string will collide with this. There are $2^{160}$possible outputs. Say there are 20,000 computers at MIT, each with 10,000 files. This means there are $\frac{2\*10^{8}}{2^{160}}$ = $1\*10^{-40}$chance there will be a collision somewhere at MIT.
3. It would take $4\*10^{34}$ years if you could do 1 million checks a second.

## Part 3

1. Sealing prevents other people from viewing the document; it completely hides the plain text. Signing indicates that the message has not changed; it appends they key to the end of the plain text.
2. 6.033-staff@mit.edu
3. Signature 2 is bad. This could mean that it was modified after it was signed. (Signature 1 has expired, by the way.)

gpg: Signature made Tue 27 Apr 2010 02:43:32 AM EDT using RSA key ID BD18CA24

gpg: BAD signature from "MIT 6.033 sp2010 (Key for hands-on #6 - Crypto) <6.033-staff@mit.edu>"

1. The message must be included in the signature! It is hashed and used in the signature. The date is also probably included. The signature is generated with the private key of the user, who indicates who signed it.
2. Chris Post <ccpost@mit.edu> signed the key. His key was signed by about 43 other keys. Depending on the legitimacy of these keys, this is a good sign that they key is valid. If I knew that Chris was a member of the course staff, I could know that the BD18CA24 key is valid.
3. The key claims to be Barack Hussein Obama (DOD) <president@whitehouse.gov>. It does not matter that you got it from the MIT key server. It matters who signed the key. The key is only self-signed.