h_2

Connor Taffe

April 16, 2016

1 C-2.6

Three keys are not dusty, the passcode is four keys long.

$$3^4 \tag{1}$$

2 C-2.11

Using an assymetric key is the most safe system. That way there is no danger in decrypting the code by reading a large number of known account numbers. Hashing the account number is very poor because the attacker can probably guess the hashing scheme.

3 R-3.3

$$1 + 2 + 4 = 7 \tag{2}$$

4 R-3.12

$$200,000 * 2^{24} \tag{3}$$

5 R-3.13

$$100 * 500,000 \tag{4}$$

6 R-3.14

Yes, because his user has read and write permissions. Another member of group `hippos` does not have read access though.

7 C-3.1

Yes it does, as the search space is now 1 instead of 2^l where l is the bit length of a random salt value.

8 C-3.2

$2^20 = 1048576$ vs $36^8 = 2821109907456$ for an 8 character password using alphanumeric characters. It is about 10^6 times weaker than a subpar password.

9 C-3.3

Kind of, it is still 2^20 since there are twenty pairs of which one is correct for a single login. But, since they are now in random order, the password cannot be stored as a single sequence of answers, so the computing power to check each pair is higher and requires a copy of each of the 20 favorite pictures to compare. So in practicality it is more difficult.