Computer Security

Assignment 1

University of Sussex
Candidate Number: 164574

Contents

1 Principles, User authentication, Malware

1.1 Task 1

1. cr@zyp@ss

    - The password cr@zyp@ss is unsuitable for computer security. The suitability of the password is that it includes nine characters in total and two of these characters are special characters. The unsuitability of the password is that it contains no upper case characters and no numbers. The special characters are a common replacement for the character 'a' and when replaced leaves two plain text dictionary words. The special characters provide minimal security and is prone to dictionary attacks and brute force.

2. qwerty

    - The password qwerty is unsuitable for computer security. The password is extremely short only being 5 characters long without any upper case characters, special characters or numbers. The word 'qwerty' is a word in the dictionary and would be highly likely to be used in a dictionary attack and will be included in common passwords. Due to its simplicity and frequency used as a password, it would be highly vulnerable to brute force attacks, common password attacks and dictionary attacks, therefore making it an extremely unsuitable password.

3. *laptop_admin#

    - The password *laptop_admin# is an unsuitable password for computer security. The password is a good length at 14 characters long and has three unique special characters. The password however includes two plain text dictionary words and the words laptop_admin will likely be included in common passwords. This password would be vulnerable to sophisticated attacks which include multiple attacks as the complexity of the password with multiple special characters would be secure against brute force attacks but would be more susceptible to dictionary and common password attacks.

4. KVK919

    (a) The password KVK919 is an unsuitable password for computer security. The password is intermediate in length as it is only six characters long however the password does not include and special characters. The password includes a mixture of upper case letters and numbers however it only includes 4 unique characters as the letter 'K' and the number '9' are repeated. This makes the password vulnerable to brute force attacks due to its length, repeated characters and lack of complexity.

1.2 Task 2

2 Digital Forensics

2.1 Task 3

3 Encryption

3.1 Task 4

3.2 Task 5

- Choose two distinct primes p and q of approximately equal size so that their product $n = pq$ is of the required bit length.

$$\begin{aligned} p &= 13 \\ q &= 31 \\ n &= 403 \end{aligned}$$

- Compute $\phi(n) = (p-1)(q-1)$.

$$\begin{aligned} p-1 &= 12 \\ q-1 &= 30 \\ \phi(n) &= 360 \end{aligned}$$

- Choose a public exponent $e, 1 < e < \phi(n)$, which is co-prime to $\phi(n)$, that is, $gcd(e, \phi(n)) = 1$.

$$gcd(e, \phi(n)) = gcd(19, 360) = 1$$

- Compute a private exponent d that satisfies the congruence $ed \equiv 1\ (mod\ \phi(n))$.
  - Suitable candidate for $1\ (mod\ \phi(n)) = 361 = 19 \cdot 19$

$$\begin{aligned} d &= 19 \\ e &= 19 \\ n &= 403 \\ \phi(n) &= 360 \\ e \cdot d &= 361 \\ e \cdot d\ mod\ \phi(n) &= 1 \end{aligned}$$

  - e and $\phi(n)$ are relatively prime
  - d and $\phi(n)$ are relatively prime

- Make the public key (n, e) available to others. Keep the private values d, p, q, and $\phi(n)$ secret.

- Encryption: cipher text, $c = RsaPublic\,(m) = m^e\ mod\ n$, where $1 < m < n-1$.

$$\begin{aligned} m &= 2 \\ 2^{19}\ mod\, 403 &= 388 \\ c &= 388 \end{aligned}$$

- Decryption: plain text, $m = RsaPrivate\,(c) = c^d\, mod\, n$.

$$\begin{aligned} c &= 388 \\ 388^{19}\, mod\, 403 &= 2 \\ m &= 2 \end{aligned}$$

4 Challenge

4.1 Task 6

4.2 Task 7

4.3 Task 8