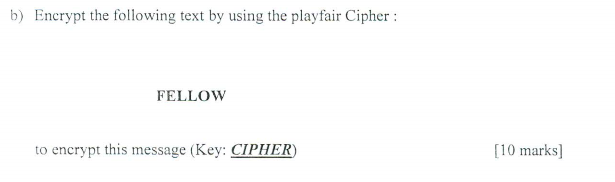


b，



playfair

Key: cipher

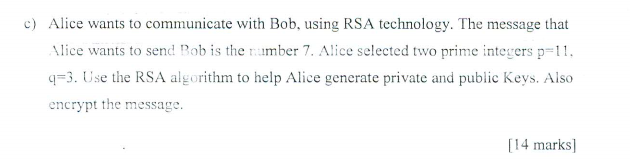
Data: follow

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C | I | P | H | E |
| R | A | B | D | F |
| G | J | K | L | M |
| N | O | S | T | U |
| V | W | X | Y | z |

Fo lx ow

Au ky wi

Fo lx ow

Send 7

11 , 3

N = 11 \* 3= 33

N\*= 10\* 2 = 20

E = 13

13x + 20y = 1

20 = 13 x 1 + 7

13 = 7 x 1 + 6

7 = 6 x 1 + 1

7 = 20 x1 + 13 \* -1

6 = 13 \* 1 + 7 \* -1

1 = 7\*1 + 6 \* -1

1 = 7 \* 2 – 13 \* 1

1 = 20 x2 – 13 \* 3

X = -3 , y = 2

D = -3

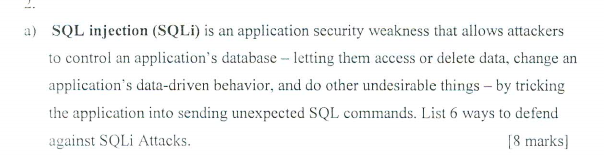
Public key 33, 13 , private key 33, -3

7^13 = c (mod 33)

C= 13

13^-3 = m (mod 33)

2



在设计应用程序时，完全使用参数化查询（Parameterized Query）来设计数据访问功能。

在组合SQL字符串时，先针对所传入的参数加入其他字符（将单引号字符前加上转义字符）。

如果使用PHP开发网页程序的话，需加入转义字符之功能（自动将所有的网页传入参数，将单引号字符前加上转义字符）。

使用php开发，可写入html特殊函数，可正确阻挡XSS攻击。

其他，使用其他更安全的方式连接SQL数据库。例如已修正过SQL注入问题的数据库连接组件，例如ASP.NET的SqlDataSource对象或是 LINQ to SQL。

使用SQL防注入系统。

增强WAF的防御力

Or

**Character Filtering**

SQL is one of the easiest ways of defending yourself against injection attacks and we can provide protection by filtering the characters in the system. As you know, mostly Sql injection attack methods use characters such as single quotes (') and filtering these characters will partially protect our system. By filtering, we can provide protection by converting one nail into double nails. The code below will work.

**Limit Record Lengths**

It is infinitely preferable that your site edit text entries according to the length of space allocated to your database. For example, if a maximum of 15 characters are entered in an entry field, no excess characters should be allowed in the field, this is a sensible precaution to take against SQL injection attacks.

**Check Record Types**

Check the types of data entered in a form that you have prepared. For example, a different type of input can be provided while the corresponding form must be entered. Such a check can be solved by writing simple codes for robustness.

**Limit Authorizations**

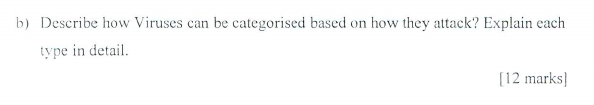
If possible, it would be an advantage for you to connect to the database with restricted privileges, rather than through connection administrator rights. This acts as a useful backstop in case your system falls prey to an injection attack, the attacker will not be able to do much without admin privileges buying you time to remediate.

**Use A Whitelist**

Everyone recommends setting up the blacklist but an attacker can override the blacklist you set up by modifying combinations. But if you set the whitelist logically, so you can avoid the bad codes and white list the good code to work.

**Use GreenSQL**

GreenSQL is an (open source and GPL license) DB Firewall application that protects the database against SQL injection attacks, it works with proxy logic and has MySQL compatibility.



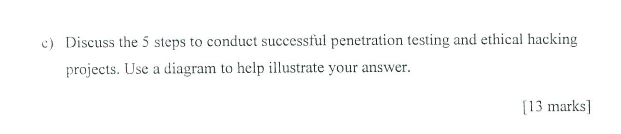
File viruses: File-infecting viruses attack executable programs, such as all files with “.exe” and “.com” extensions.

Script viruses: Script viruses are a subset of file viruses, written in a variety of script languages (VBS, JavaScript, BAT, PHP, etc.). They either infect other scripts ( for example, Windows or Linux command and service files), or form a part of multi-component viruses. Script viruses are able to infect other file formats, such as HTML, if the file format allows the execution of scripts.

Boot viruses: Boot viruses attack boot sectors (removable media boot sector or hard disk master boot sector) and set their own loading routines at start-up

Macro viruses: Macro viruses attack documents where other commands (macros) can be inserted. These viruses are often embedded within word processing or spreadsheet applications, since macros are easily inserted into these types of files.

C.



<https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking>

1. Reconnaissance:
2. Scanning:
3. Gaining Access:
4. Maintaining Access:
5. Clearing Track:

3.a.



If the size of the original file is already known or estimated then that could be a potential threat to the excess of the memory that it would show in its properties

If the decrypting JavaScript has been exploited or destroyed or meddled with then the information that had been sent could be safely considered as lost or irrevocable

If the passphrase for the steganography utility as in the steghide utility for Linux based platform is compromised or lost or forgotten then again extraction of the hidden content would be nearly impossible .

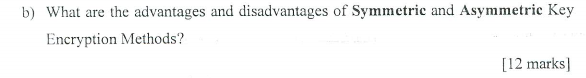
Also steganography is a concept that has been known for quite a while ever since al Qaeda used it for the 9/11 and has been widely worked upon . This in turn means that there would be several ways through which the confidentiality of the hidden file could be compromised or the hidden data could fall into the undesirable hands . People would have figured it out already and hence this method of encryption would be archaic and commonplace

太过时了

如果数据被修改很难恢复

必须2个互相信任之间的通信

[https://www.quora.com/What-are-steganography-disadvantages`](https://www.quora.com/What-are-steganography-disadvantages%60)

b. <http://techrejects.blogspot.com/2014/08/advantages-disadvantages-symmetric-asymmetric-key-encryption-methods.html>

**Symmetric Key Encryption**

**Advantages**

- **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.

- **Encrypt and decrypt your own files:** If you use encryption for messages or files which you alone intend to access, there is no need to create different keys. Single-key encryption is best for this.

- **Fast:** Symmetric key encryption is much faster than asymmetric key encryption.

- **Uses less computer resources:** Single-key encryption does not require a lot of computer resources when compared to public key encryption.

- **Prevents widespread message security compromise:** A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

**Disadvantages**

- **Need for secure channel for secret key exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.

- **Too many keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.

- **Origin and authenticity of message cannot be guaranteed:** Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

**Asymmetric/Public Key Encryption**

**Advantages**

- **Convenience:** It solves the problem of distributing the key for encryption.Everyone publishes their public keys and private keys are kept secret.

- **Provides for message authentication:** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.

- **Detection of tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.

- **Provide for non-repudiation:** Digitally signing a message is akin to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

**Disadvantages**

- **Public keys should/must be authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

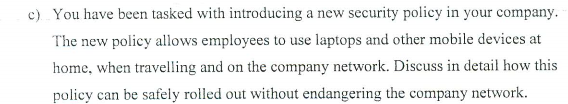
- **Slow:** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.

- **Uses up more computer resources:** It requires a lot more computer supplies compared to single-key encryption.

- **Widespread security compromise is possible:** If an attacker determines a person's private key, his or her entire messages can be read.

- **Loss of private key may be irreparable:** The loss of a private key means that all received messages cannot be decrypted.

c.

 <https://www.techradar.com/news/networking/wi-fi/five-tips-for-a-secure-wireless-network-1161225>

Use stronger encryption. ...

Use a secure WPA password. ...

Check for rogue Wi-Fi access points. ...

Provide a separate network for guests. ...

Hide your network name. ...

Use a firewall. ...

Enable MAC authentication for your users. ...

Use a VPN.