EE6102 SUMMARY

Crber security level网络安全等级

1.现状：工业 4.0（industry 4.0）和数字转型（digital transformation）带来了更多数字资产，使得更容易受到网络攻击。

2.防护措施

（1）技术解决：Cryptography, firewalls, software updates, use strong passwords and two factor authentication, regular backup密码学、防火墙、软件更新、使用强密码和双因素认证、定期备份

（2）非技术解决：

provide regular security training for employees to help them identify potential threats and be cautious when clicking on links or downloading attachments from unknown sources.为员工提供定期安全培训以帮助他们识别潜在威胁，并在点击链接或从未知来源下载附件时保持谨慎

3.未来：总是存在网络安全攻击。更多的保护将减少成功攻击的可能性

4.防护的目标：

CIA：（1）**Confidentiality机密性**：means to prevent the unauthorized access/sharing of data.是指防止未经授权的访问/共享数据。

（2）**Integrity完整性**： means data must not be changed by unauthorized people.完整性意味着未经授权的人员不得更改数据。

（3）**Availability可用性**： means information should be consistently and readily accessible for authorized parties.可用性意味着信息应始终如一地可供授权方随时访问。

Authentication 身份验证：Assurance that communicating entity is the one claimed.保证通信实体是所声明的实体。

Privacy 隐私性：

Non-repudiation 不可否认性：Protection against denial by one of the parties in a communication.防止通信中的一方否认

恶意软件malware

总体描述: Any malicious software which has been written to cause harm.编写用于造成伤害的一切恶意软件

virtus病毒：Virus is malicious program that replicates itself and infects computers, however it needs a host to travel.病毒是自我复制并感染计算机的恶意程序，需要主机才能传播。

worm蠕虫：Worm doesn’t require a host蠕虫不需要主机。

logic bomb逻辑炸弹：当满足某些条件时，表现得像病毒，执行恶意行为

bonets僵尸网络：Botnet is a network of computer zombies (bots controlled by a master). It can be used to launch denial of service (DOS) attacks, which can cripple a server or network by sending out excessive traffic. It also can be used to crack password in addition to launch many types of other attacks.僵尸网络是一种由计算机僵尸（受主控的机器人）组成的网络。它可以用来发起拒绝服务（DOS）攻击，通过发送过多的流量使服务器或网络瘫痪。此外，

它还可以用来破解密码以及发起许多其他类型的攻击。（安装了恶意代码的计算机网络）

trojan木马：The trojan disguises itself as legitimate software, however it is a malicious software that might install adware, keylogger or open a backdoor.该木马伪装成合法软件，但其实是一种恶意软件，可能会安装广告软件、键盘记录器或打开后门。

ransomware勒索软件：Ransomware blocks access to the network's key components until you pay (normally using Bitcoin), and in some cases you may not be granted access even after the payment.勒索软件会阻止对网络关键组件的访问，直到您付款（通常使用比特币），在某些情况下，即使在付款后您也可能没有被授予访问权限。

Spyware间谍软件： software that steals all your confidential data without your knowledge. 在你不知情的情况下窃取你所有机密数据的软件

adware广告软件：software that displays advertising content such as banners on a user's screen.在用户的屏幕上显示广告内容的软件

rootkit：Rootkit is a set of programs that allows someone to gain control over systems and hides the fact that the computer has been compromised. Very difficult to detect as it masks behaviors of other malwares.Rootkit是一组程序，允许某人获得对系统的控制，并隐藏计算机已被破坏的事实。由于它掩盖了其他恶意软件的行为，因此很难检测到。

如何防御恶意软件攻击：

（1）Use antivirus software. It can protect your computer against malware.

（2）Use firewalls. Windows and Mac OS have their default built-in firewalls, named Windows Firewall and Mac Firewall.

（3）Avoid clicking on suspicious links.

（4）Update your OS and browsers, regularly

网络钓鱼phishing attack

社会工程学：manipulating people so that they end up giving their confidentialinformation.操纵人们，让他们最终泄露自己的机密信息。

描述:an attacker impersonates to be a trusted contact and sends the victim fake mails.By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.攻击者冒充可信联系人向受害者发送虚假邮件。攻击者可以获取机密信息和账户凭证。他们还可以通过网络钓鱼攻击安装恶意软件。

类型：Spear 鱼叉式(针对特定个人或群体)，Whaling 鲸式(专门针对公司中最关键的人物,向同事索取个人或公司信息)，Smishing 短信钓鱼，Vishing 电话钓鱼，Angler phishing 垂钓者网络钓鱼

如何防御：

（1）Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.仔细检查您收到的电子邮件。大多数网络钓鱼电子邮件都存在重大错误，例如拼写错误和与合法来源的格式更改。

（2）Make use of an anti-phishing toolbar. 利用反网络钓鱼工具栏

（3）Update your passwords regularly. 定期更新您的密码。

（4）Conduct regular employee training. 定期进行员工培训。

（5）Stay up-to-date with security patches and updates. 及时了解安全补丁和更新。

密码攻击password attack

类型：（1）Brute attack暴力攻击：Trial and error method used to decode the password or data用于解码密码或数据的试错法

（2）Dictionary attack字典攻击：Use every password that is possible through the dictionary 使用字典中可能的所有密码

（3）Rainbow attack：Attacker use hash tables to find the password of the user攻击者使用哈希表查找用户的密码 找到相似的

如何防御：

（1）Use strong alphanumeric passwords with special characters

（2）Refrain from using the same password for multiple websites or accounts.

（3）Update your passwords (advisable to changed it every 90 days); this will limit your exposure to a password attack.

（4）Do not have any password hints in the open.

Role of Multi-Factor Authentication (MFA)多因素身份验证：

（1）Multi-Factor Authentication is a security system that requires users to provide two or more verification factors to gain access to a resource. It adds extra layers of security beyond just a password.

（2）MFA means more than one authentication factors. Password is permanent, and temporary authentication from SMS/app can reduce attacks. Because attackers do not have access to physical devices. So it can improve security

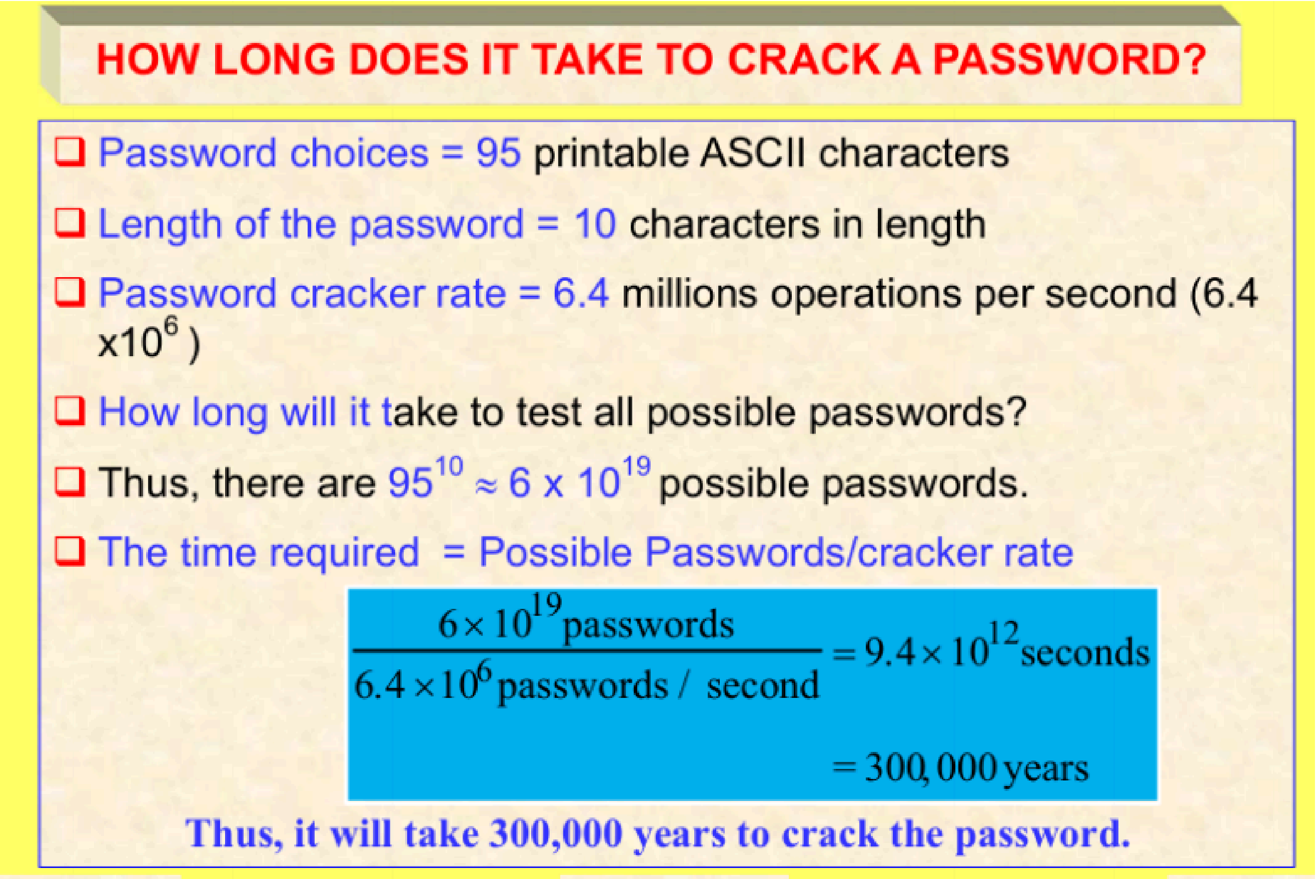
password-based authentication

优点：easy to use/ reusable / built in system / free /can be changed to regain security

缺点：can be cracked / careless / not use strong password / difficult to remember

计算：

$$Thetimerequired = PossiblePassword/crackerrate$$



HOW LONG DOES IT TAKE TO CRACK A PASSWORD?

□ Password choices = 95 printable ASCII characters

□ Length of the password = 10 characters in length

□ Password cracker rate = 6.4 millions operations per second (6.4 x10^6)

□ How long will it take to test all possible passwords?

□ Thus, there are $95^{10} \approx 6 \times 10^{19}$ possible passwords.

□ The time required = Possible Passwords/cracker rate

$$\frac{6\times 10^{19}\text{passwords}}{6.4\times 10^{6}\text{passwords / second}} = 9.4\times 10^{12}\text{seconds}$$

$$= 300{,}000\ \text{years}$$

Thus, it will take 300,000 years to crack the password.

中间人攻击man in middle attack

描述： In the Man-in-the-Middle Attack (MITM) (also known as an eavesdropping attack), an attacker comes in between a two-party communication, i.e.the attacker hijacks the session between a client and host. The client-server communication is cut off, and instead, the communication line goes through the hacker, so that they can steal or manipulate the data. 在中间人攻击 （MITM） （也称为窃听攻击）中，攻击者介于两方通信之间，即攻击者劫持了客户端和主机之间的会话，客户端与服务器之间的通信被切断，通信线路转而通过黑客，这样黑客就可以窃取或篡改数据。

如何防御：

（1）Be mindful of the security of the website.

（2）Use encryption on your devices.

（3）Refrain from using public Wi-Fi networks

SQL Injection attack

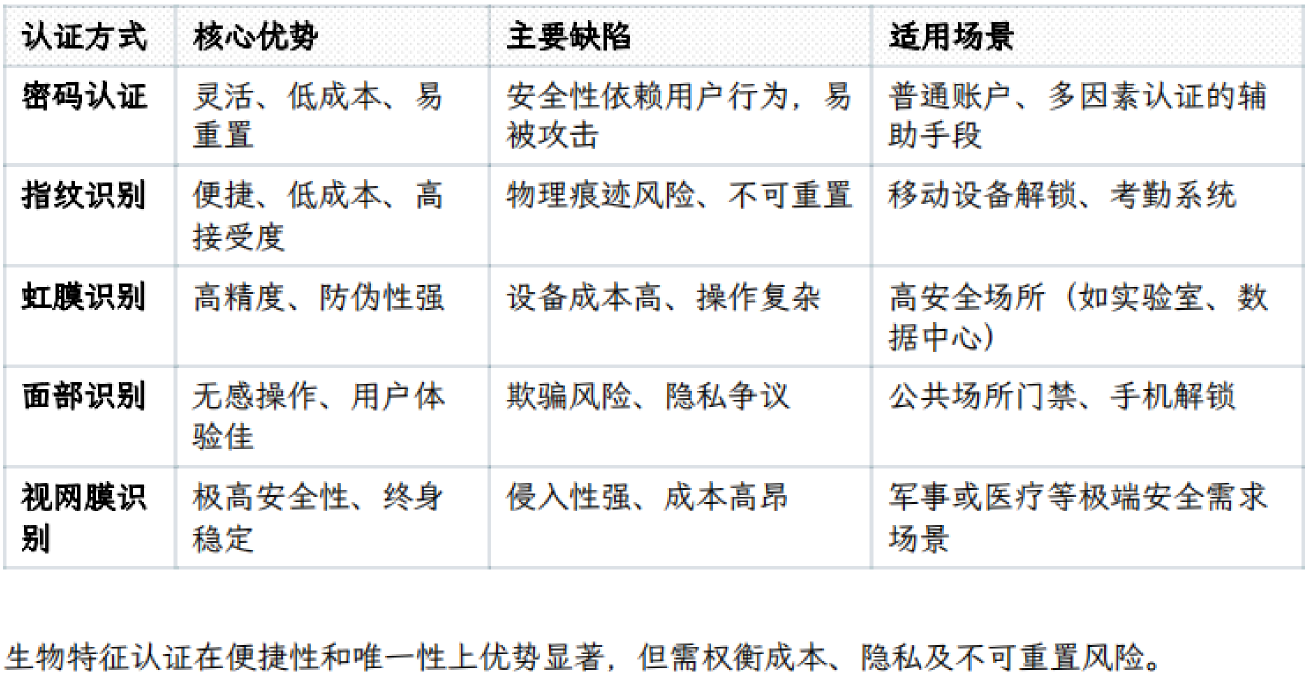
描述：It is carried by injecting a malicious code into a vulnerable website search box,thereby making the server reveal crucial information. This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this attack.通过向易受攻击的网站搜索框注入恶意代码，使服务器泄露关键信息。□这使得攻击者能够查看、编辑和删除数据库中的表。攻击者还可以通过此攻击获得管理员权限。

如何防御： （1）Use an Intrusion detection system, as they are designed to detect unauthorized access to a network.

（2）Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

biometric-based authentication(passwordless authentication)

描述：Biometric-based Authentication refers to the cyber security procedure that involves using biological characteristics of individuals such as retina, iris, voice,facial characteristics, fingerprints etc. to verify people are who they claim to be基于生物特征的身份验证是指使用个人的生物特征，如视网膜、虹膜、声音、面部特征、指纹等，来验证人们是否是他们声称的人的网络安全程序。
如何工作：
优点：Difficult to hack / convenient / always available
缺点：（1）The biometric type is not 100% secure. Only DNA can replace password, but it takes time and it is expensive.So we can not replace password-based authentication by biometric-based authentication.
（2）High risks:Password can be changed but biometric details can not
（3）Duplication/Cloning: Biometric credentials are easier to obtain and duplicate than access cards or keys
为什么没有替代password-based authentication？not 100%secure



认证方式	核心优势	主要缺陷	适用场景
密码认证	灵活、低成本、易重置	安全性依赖用户行为，易被攻击	普通账户、多因素认证的辅助手段
指纹识别	便捷、低成本、高接受度	物理痕迹风险、不可重置	移动设备解锁、考勤系统
虹膜识别	高精度、防伪性强	设备成本高、操作复杂	高安全场所（如实验室、数据中心）
面部识别	无感操作、用户体验佳	欺骗风险、隐私争议	公共场所门禁、手机解锁
视网膜识别	极高安全性、终身稳定	侵入性强、成本高昂	军事或医疗等极端安全需求场景

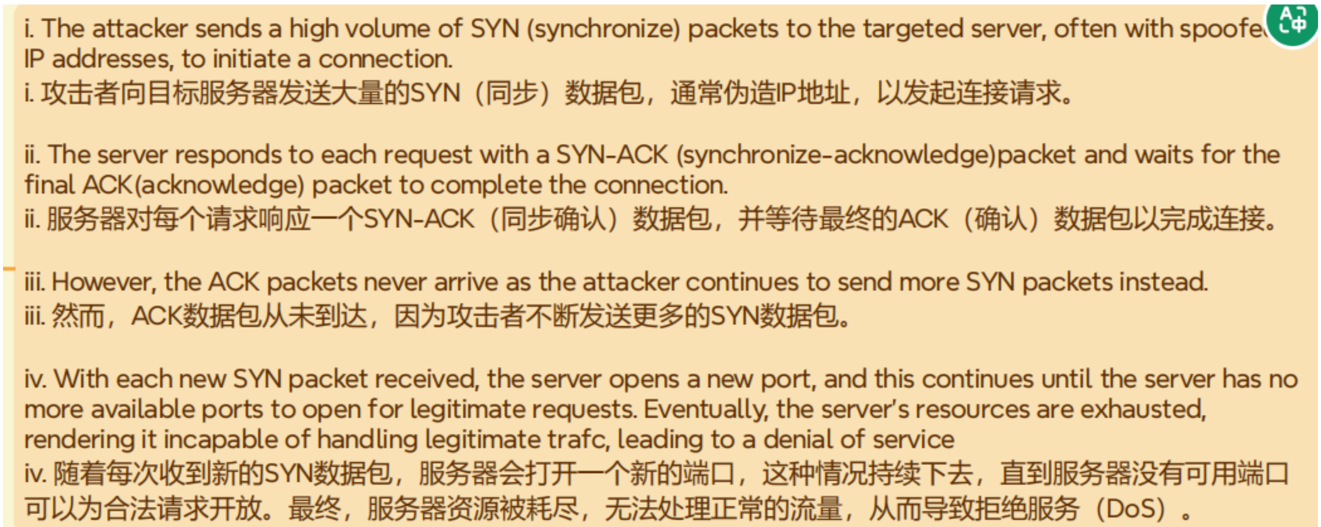
生物特征认证在便捷性和唯一性上优势显著，但需权衡成本、隐私及不可重置风险。

Denial of serivce拒绝服务攻击

DOS：attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth or crashes their system.攻击者以系统、服务器或网络为目标，用流量淹没它们，以耗尽他们的资源和带宽或使他们的系统崩溃。
DDOS: DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.当攻击者使用多个受感染的系统发起此攻击时，它也被称为 DDoS（分布式拒绝服务）攻击。

SYN flood attack：In a TCP SYN flooding attack, an attacker uses bots to flood a server with TCP connection-opening (SYN) requests. A server reserves a certain amount of capacity each time it receives a SYN segment.Flooding a server with SYN segments can cause the server to run out of resources and crash or be unable to open valid requests. A SYN flood can shut down an entire network if strong enough.在TCP SYN洪泛攻击中，攻击者利用机器人向服务器发送大量TCP连接建立（SYN）请求。每当服务器接收到一个SYN段时，会预留一定数量的资源。用SYN段淹没服务器会导致服务器资源耗尽，从而崩溃或无法处理有效的请求。如果强度足够大，SYN洪泛可以关闭整个网络。

SYN 如何工作:



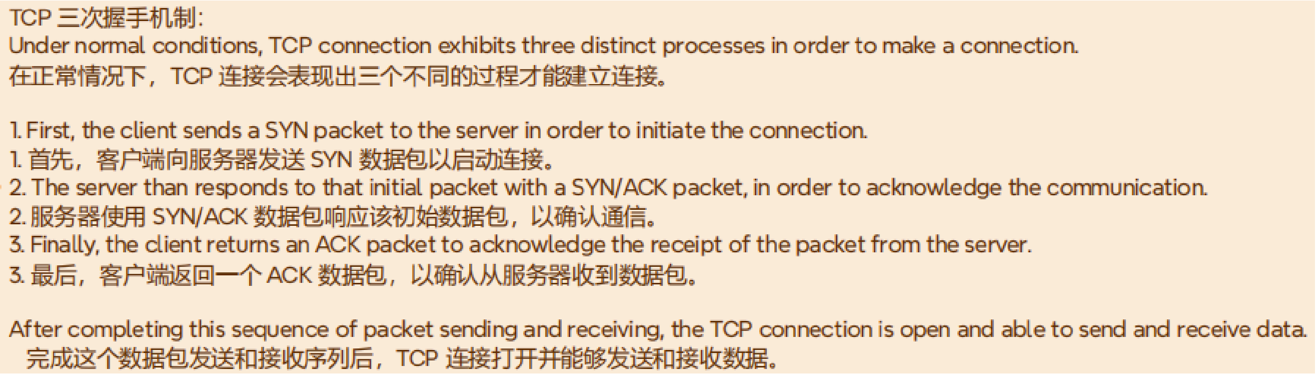
i. The attacker sends a high volume of SYN (synchronize) packets to the targeted server, often with spoofe
IP addresses, to initiate a connection.
i. 攻击者向目标服务器发送大量的SYN（同步）数据包，通常伪造IP地址，以发起连接请求。

ii. The server responds to each request with a SYN-ACK (synchronize-acknowledge)packet and waits for the final ACK(acknowledge) packet to complete the connection.
ii. 服务器对每个请求响应一个SYN-ACK（同步确认）数据包，并等待最终的ACK（确认）数据包以完成连接。

iii. However, the ACK packets never arrive as the attacker continues to send more SYN packets instead.
iii. 然而，ACK数据包从未到达，因为攻击者不断发送更多的SYN数据包。

iv. With each new SYN packet received, the server opens a new port, and this continues until the server has no more available ports to open for legitimate requests. Eventually, the server's resources are exhausted, rendering it incapable of handling legitimate trafc, leading to a denial of service
iv. 随着每次收到新的SYN数据包，服务器会打开一个新的端口，这种情况持续下去，直到服务器没有可用端口可以为合法请求开放。最终，服务器资源被耗尽，无法处理正常的流量，从而导致拒绝服务（DoS）。

SYN如何发布:



TCP 三次握手机制:
Under normal conditions, TCP connection exhibits three distinct processes in order to make a connection.
在正常情况下，TCP 连接会表现出三个不同的过程才能建立连接。

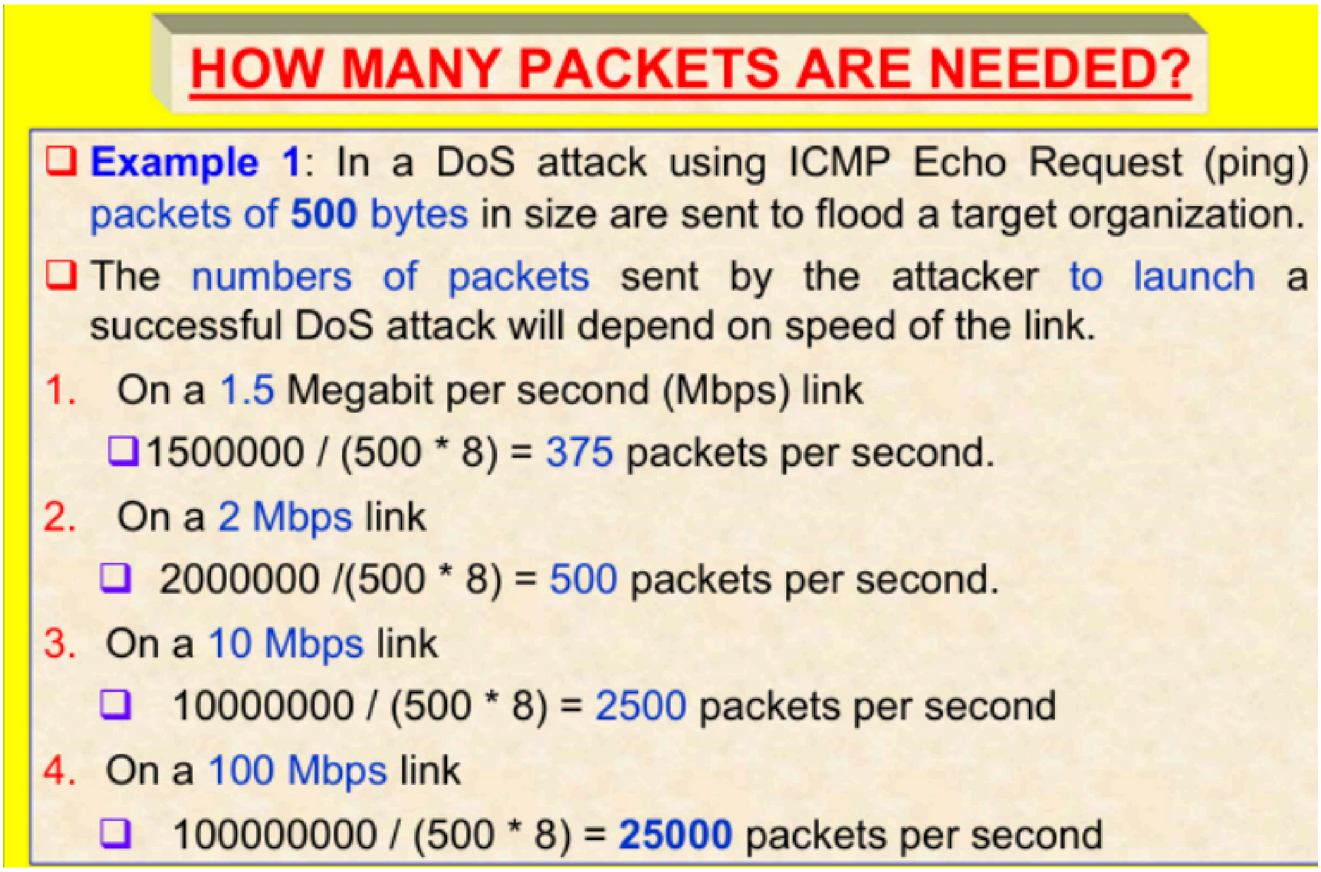
1. First, the client sends a SYN packet to the server in order to initiate the connection.
1. 首先，客户端向服务器发送 SYN 数据包以启动连接。
2. The server than responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.
2. 服务器使用 SYN/ACK 数据包响应该初始数据包，以确认通信。
3. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server.
3. 最后，客户端返回一个 ACK 数据包，以确认从服务器收到数据包。

After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.
完成这个数据包发送和接收序列后，TCP 连接打开并能够发送和接收数据。

DOS计算:

$$numberofpackets = speedoflink/packetssize(byte)*8$$

Example:



HOW MANY PACKETS ARE NEEDED?

❑ Example 1: In a DoS attack using ICMP Echo Request (ping) packets of 500 bytes in size are sent to flood a target organization.

❑ The numbers of packets sent by the attacker to launch a successful DoS attack will depend on speed of the link.

1. On a 1.5 Megabit per second (Mbps) link
   ❑ 1500000 / (500 * 8) = 375 packets per second.
2. On a 2 Mbps link
   ❑ 2000000 /(500 * 8) = 500 packets per second.
3. On a 10 Mbps link
   ❑ 10000000 / (500 * 8) = 2500 packets per second
4. On a 100 Mbps link
   ❑ 100000000 / (500 * 8) = 25000 packets per second

包大小的影响：同带宽下：包越大，发动攻击需要的数据包数量越少；包越小，发动攻击需要的数据包数量越大

带宽的影响：：带宽越大，能容纳更多的数据包；带宽较低时，少量的数据包也可能导致DOS。

DNS flood attack：

僵尸网络如何帮助DDOS:因为他们安全性都比较差，很容易被攻击者控制并组建僵尸网络

DNS flood attack: a type of DDoS attack that targets the Domain Name System (DNS), which translates between easy to remember names (e.g.,example.com) and hard to remember addresses of website servers (e.g.,192.168.0.1), so successfully attacking DNS makes the Internet unusable for most people.DNS洪水攻击： 一种针对域名系统（DNS）的分布式拒绝服务（DDoS）攻击。DNS负责将易于记忆的名称（例如 example.com）转换为网站服务器的难以记忆的地址（例如 192.168.0.1）。成功攻击DNS会使大多数人无法使用互联网，从而造成大规模的网络瘫痪

DNS如何工作：DNS flood attacks use the high bandwidth connections of IP cameras, DVR boxes and other IoT devices to directly overwhelm the DNS provider’s services. The only way to withstand these types of attacks is to use a very large and highly distributed DNS system that can monitor, absorb, and block the attack traffic in real time.DNS 洪水攻击利用 IP 摄像机、DVR 盒和其他物联网设备的高带宽连接，直接压垮 DNS 提供商的服务。抵御这些类型攻击的唯一方法是使用非常大且高度分布式的 DNS 系统，该系统可以实时监控、吸收和阻止攻击流量。

如何防御DDOS:

(1)Run a traffic analysis to identify malicious traffic

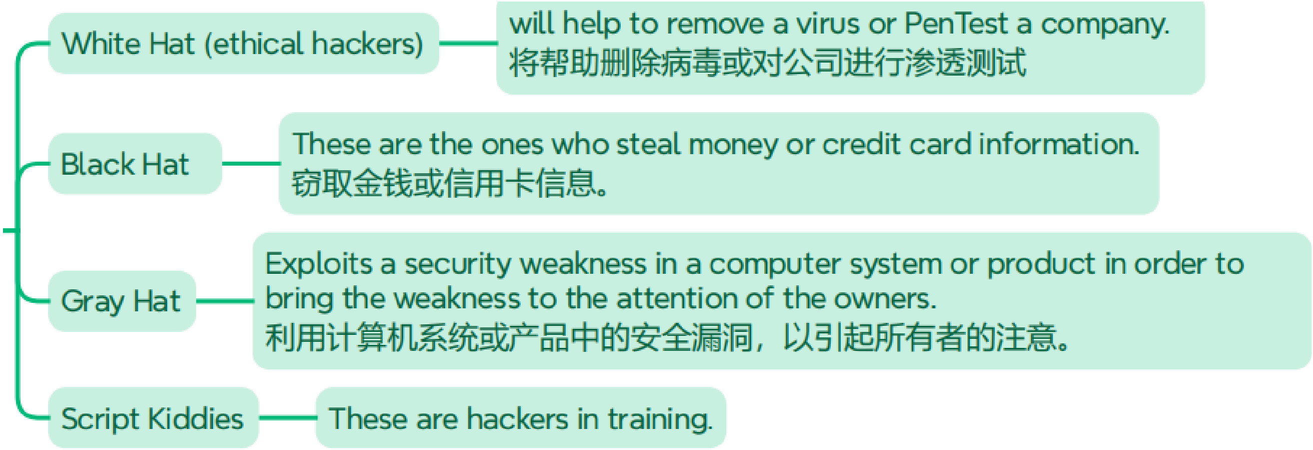
(2)Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.

(3)Formulate an incident response plan, have a checklist and make sure your team and data center can handle a DDoS attack.
(4)Outsource DDoS prevention to cloud-based service providers (Cloudflare,NETSCOUT, Akamai, AWS, etc.).

inside threat内部威胁

描述：it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.
原因：greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.
如何防御：
（1）Organizations should have a good culture of security awareness.
（2）Companies must limit the IT resources staff can have access to depending on their job roles.
（3）Organizations must train employees to spot insider threats

黑客



White Hat (ethical hackers) — will help to remove a virus or PenTest a company. 将帮助删除病毒或对公司进行渗透测试

Black Hat — These are the ones who steal money or credit card information. 窃取金钱或信用卡信息。

Gray Hat — Exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. 利用计算机系统或产品中的安全漏洞，以引起所有者的注意。

Script Kiddies — These are hackers in training.

网络安全规划

信息安全的两个方面：技术（technical）和管理（managerial）
安全策略：
（1）自上向下： 明确的政策、充足的预算、持续的支持及保护流程。
优点：Strong upper management support；Dedicated funding；Clear planning and chance to influence organizational culture
缺点: issue policy, procedures, and processes；Dictate the goals and expected outcomes of the project；Determine who is accountable for each required action
（2）自下向上： 由于缺少参与者支持和组织持久力，难以成功
优点：Technical expertise of the individual administrators
缺点：Participant support，Organizational staying power
Digital Liability Management (DLM): Also known as “The Intersection of Policy and

Technology”, focuses on the intersection of policy and technology
网络安全策略：Zero Trust Security + Defense In Depth

SSL,SET

Secure Socket Layer (SSL) is a method where transactions using a Web browser is encrypted. SSL protects the transmission but does not authenticate the sender. On the other hand
Secure Electronic Transaction (SET) authenticates consumer, merchants and all parties during the transactions.
SET安全但是没有使用的原因： （1）Need to install SET software on client computers
（2）Cost and complexity for merchants to offer support for SET compared to low cost and simplicity of the SSL.
（3）Client-side certificate distribution logistics.
（4）SET was difficult to use while SSL was easy to use and built in all popular browsers.

Cryptography密码学

1.密码学的描述：

Cryptography is the process of encrypting information through algorithms so that unauthorized people cannot view it.密码学就是通过算法对信息进行加密，使得未经授权的人无法查看信息。

2.密码学如何提供安全性：

使用数学运算来保护在各方之间传输或存储在计算机上的消息。它涉及将消息从可读格式转换为不可读格式，加密和解密信息以防止未经授权的访问。发送方和接收方都应该知道解密过程。

3.密钥长度在密码学中的作用

For the same algorithm, the longer the key length, the stronger the encryption.对于同一个算法而言，密钥长度越长，加密性越强。（安全性=密码强度+密码长度）

```
对于密码学，用于基于密码的身份验证时建议使用长密钥，但在ATM机上只用4-6位的PIN码，安全吗？回答：Passwords can be entered automatically, and the system can be tricked to allow unlimited attempts. Normally, the attacker will take over millions of compromised computers and with fast connections, this task of cracking a cryptography password can be accomplished within few seconds.The ATM card’s PINs must be entered manually, after three unsuccessful attempts, ATM card will be taken by the machine.Since the attacker must be physically present at an ATM machine, if caught, the local law will apply, and the attacker will be punished. For the above reasons, it is easy for attackers to crack long passwords, compared to short ATM pins.密码可以自动输入，系统可以被
```

> 欺骗，允许无限次的尝试。通常情况下，攻击者将接管数百万台受损的计算机，并且通过快速连接，破解加密密码的任务可以在几秒钟内完成。ATM卡的密码必须手动输入，三次输入不成功后，ATM卡将被机器取走。由于攻击者必须亲自出现在ATM机上，如果被抓住，当地法律将适用，攻击者将受到惩罚。由于上述原因，与短的ATM引脚相比，攻击者更容易破解长密码。

4.secret key cryptography私钥加密（对称加密）（one key）

描述： 使用单一密钥进行加密和解密，双方共享同一密钥。代表算法AES、DES。
优点：

- 速度快，适合处理大量数据；安全；密钥短
- 实现简单，计算资源消耗低
- 可有效用于数据存储保护
  缺点：
- 密钥分发困难（密钥必须保持机密）
- 密钥管理复杂（多人共享易泄露）Key management is complex (sharing among multiple people is prone to leakage)
- 无法验证发送方身份
- 如果密钥丢失了，加密系统失效

5.public key cryptography公钥加密（非对称加密）（two keys）

描述： 使用一对密钥，用公钥加密后，只能用相应的私钥解密，必须成对使用。代表算法：RSA、ECC。
优点：

- 解决密钥交换问题（公钥可公开）
- 支持数字签名（私钥签名，公钥验证）
- 身份认证强
  缺点：
- 计算复杂，速度慢（不适合大数据加密）
- 密钥长度长（资源消耗高）
- 依赖数学难题安全性（如质因数分解）

6.hashing（哈希，单向加密）（不使用key）

描述： 将任意长度输入转换为固定长度输出（哈希值），不可逆（can't de-hash)。代表算法：SHA-256、MD5。
如何提供完整性： 一旦算法被处理，就没有可行的方法来使用密文来检索明文。没有可行的方法可以生成两个计算相同哈希值的不同明文
在数字签名中的作用： It provide security and efficiency. 提供了安全性和效率。

- Efficiency：it doesn’t encrypt whole message. It only encrypt hash, which make it faster. 不需要加密整个信息，只加密哈希值。

- Security : when sending message with digital signature, we don't encrypt message. We can only compare hash to see whether the message has been changed when verifying digital signature.当用数字签名发送信息时，不需要加密信息内容，只需要在验证数字签名时对比哈希值是否被篡改即可
  优点:
- 确保数据完整性（篡改后哈希值变化）
- 快速计算
- 无需密钥管理
  缺点:
- 无法还原原始数据
- 存在哈希碰撞风险There is a risk of hash collision
- 不提供加密功能

7.数字签名和数字证书

数字签名: Digital signing is used to provide trust that the content has come from the claimed source and has not been altered数字签名用于提供内容来自声明的来源且未被更改的信任。
数字证书: For digital signatures to work, a trusted third party known as a Certification Authority (CA) is needed to issue digital certificates that certify the electronic identities and public keys of users and organizations.要使数字签名正常工作，需要一个称为证书颁发机构（CA）的受信任的第三方来颁发数字证书，以证明用户和组织的电子身份和公钥。
如何工作:

- 产生：只有私钥持有者才能使用私钥对信息进行签名，签名将变成信息的一部分（私钥加密，公钥解密）
- 验证：任何匹配公钥的持有者可以验证签名。
  确保完整性：任何改变都会被message digest algorithm检测出

8.RSA

如何工作：用户选择两个大素数p,q,计算模数N=p*q，计算 ϕ(n)=(p-1)(q-1)用于计算私钥。选择公钥e，要保证e是质数而且e和ϕ(n)互质，且e小于ϕ(n)，大于1。令*ed mod ϕ(n) = 1来计算私钥d，实际上是利用k(变量)乘ϕ(n)然后+1再除e算得的d。然后把N和e告诉对方。对方利用M^e mod N 得到密文，自己利用C^d mod N来解密。
为什么选择大的质数：如果选择的质数很小，则不再安全。很容易被攻击者攻破。
优点：easy / simple / based on prime / solve exchange problem
缺点：slower than ECC（在同样的安全性下，ECC用更短的密钥）
non-repudiation不可否认性：您不能拒绝对消息进行签名，因为它是使用您的私有密钥签名的。
Authentication 身份验证：We use a digital signature algorithm to produce the signature from the hash value and the private key.我们使用数字签名算法从哈希值和私钥生成签名。The message can now be authenticated with the public key and the signature.现在可以使用公钥和签名对消息进行身份验证。

9.ECC椭圆曲线加密

相比于RSA的优点：同等安全性下，ECC密钥更短；计算高效
未来展望：相比 ECC，RSA 的密钥更长，处理速度慢，消耗计算资源，ECC正在逐渐被ECC替代，尤其在TLS1.3,区块链，以太坊，但未来可能会被Quantum computing替代由于安全性。

10.DIFFIE-HELLMAN

发展的原因：解决密钥交换问题
如何工作：找到一个素数p和原根g。用户A选择一个私钥XA<p,计算出公钥YA=g^XA mod p.用户B选择一个私钥XB<p,计算出公钥YB=g^XB mod p,然后相互发送公钥。用户 A 又生成一个密钥 KA = YB^XA mod p，用户 B 又生成一个密钥 KB = YA^XB mod p，这里的 KA = KB。用户 A 和 B 就拥有
了同样的私钥 K。
安全性：攻击者无法从公开的公钥中获取私钥
Ephemeral Diffie-Helman(EDH):每次选择的质数和生成器都不一样；所有数都是暂时的，给攻击者用于破解的时间更短。
为什么TL1.3用的是EDH而不是RSA:. RSA中的私钥是永久的，风险更大。

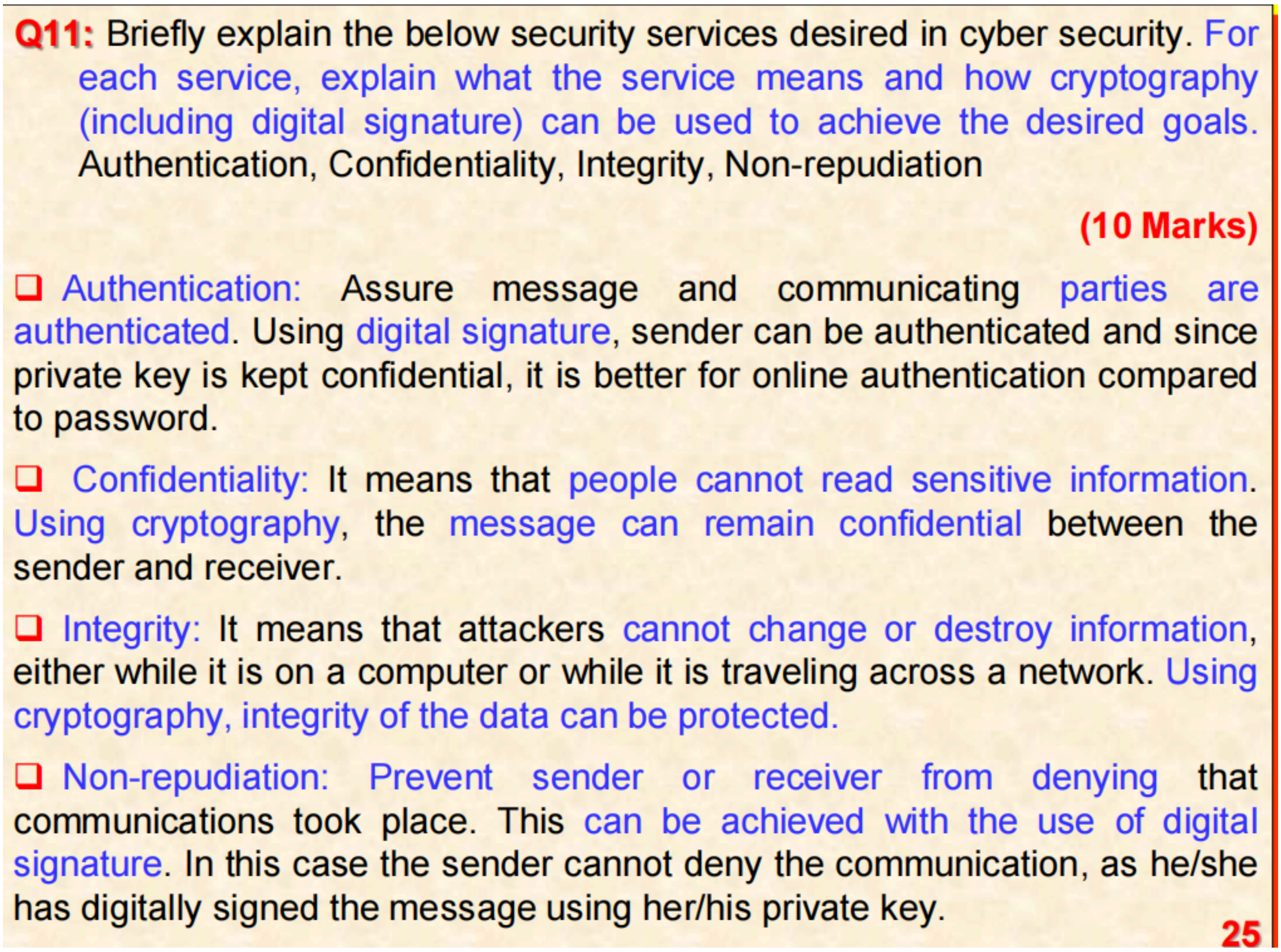
11.加密解决的在线网络安全的四个维度

（1）**integrity完整性**：It can provide assurance that the message has not been altered可确保信息未被篡改
（2）**nonrepudiation不可否认性**：Prevent the user from denying that he/she has sent the message防止用户否认已发送消息
（3）**authentication身份验证**：Provide verification of the identity of the message提供消息身份验证
（4）**confidentiality保密性**：Gives assurance that the message has not been read by others确保消息未被其他人读取

12.解释数字签名和哈希摘要为公钥加密增加了哪些方面，以及它们是如何工作的?

（1）数字签名和哈希摘要在与公钥加密结合使用时，增加了认证、不可否认性和完整性。
（2）发送者使用其私钥加密消息以生成数字签名。
（3）为了确保消息在传输过程中未被篡改，首先使用哈希函数创建消息的摘要。

13.密码学如何实现网络安全目标



Q11: Briefly explain the below security services desired in cyber security. For each service, explain what the service means and how cryptography (including digital signature) can be used to achieve the desired goals. Authentication, Confidentiality, Integrity, Non-repudiation

(10 Marks)

□ Authentication: Assure message and communicating parties are authenticated. Using digital signature, sender can be authenticated and since private key is kept confidential, it is better for online authentication compared to password.

□ Confidentiality: It means that people cannot read sensitive information. Using cryptography, the message can remain confidential between the sender and receiver.

□ Integrity: It means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Using cryptography, integrity of the data can be protected.

□ Non-repudiation: Prevent sender or receiver from denying that communications took place. This can be achieved with the use of digital signature. In this case the sender cannot deny the communication, as he/she has digitally signed the message using her/his private key.

25

Blockchain technology区块链技术

1. Blockchain technology描述：

Blockchain technology is a decentralized and distributed digital ledger that records transactions in a secure and tamper-proof way. The technology uses cryptographic algorithms to validate and verify transactions, creating a permanent and immutable record that is accessible to all network participants.
区块链技术是一种去中心化、分布式的数字账本，以安全、防篡改的方式记录交易。该技术使用加密算法来验证和验证交易，创建所有网络参与者都可以访问的永久且不可变的记录。

2. Blockchain technology主要类型

（1）**Public Blockchain公有区块链**: A public blockchain is open to everyone and allows anyone to participate in the network. Bitcoin and Ethereum are examples of public blockchains.
公有区块链向所有人开放，允许任何人参与网络。比特币和以太坊就是公有区块链的例子。
优点： Decentralization, high security, and transparency.去中心化、高安全性和透明度。
缺点： Scalability issues and slower transaction speeds.可扩展性问题和较慢的交易速度。
（2）**Private Blockchain私有区块链**: A private blockchain is restricted to a specific group of participants, and access is controlled by a central authority. Private blockchains are often used by businesses and organizations for internal purposes.
私有区块链仅限于特定的参与者群体，访问由中央机构控制。私有区块链常被企业和组织用于

内部目的。
优点： Enhanced privacy, scalability, and efficiency.增强隐私、可扩展性和效率。
缺点： Centralization risks and limited transparency.集中化风险和透明度有限。

（3）**Consortium Blockchain联盟区块链**: A consortium blockchain is a type of private blockchain where the participants are known and trusted. Consortium blockchains are often used in industries such as finance, supply chain, and healthcare.
联盟区块链是一种私有区块链，其中参与者是已知且可信的。联盟区块链通常应用于金融、供应链和医疗保健等行业。
优点： Shared control among organizations, balancing efficiency and security.组织之间共享控制权，平衡效率和安全性。
缺点： Requires cooperation and governance frameworks.需要合作和治理框架

3.Blockchain technology计算

（1）Compute Transactions per Second (TPS)

$$TPS = Transactionsperblock/time(seconds)$$

（2）Calculate Transactions per Block (TPB)

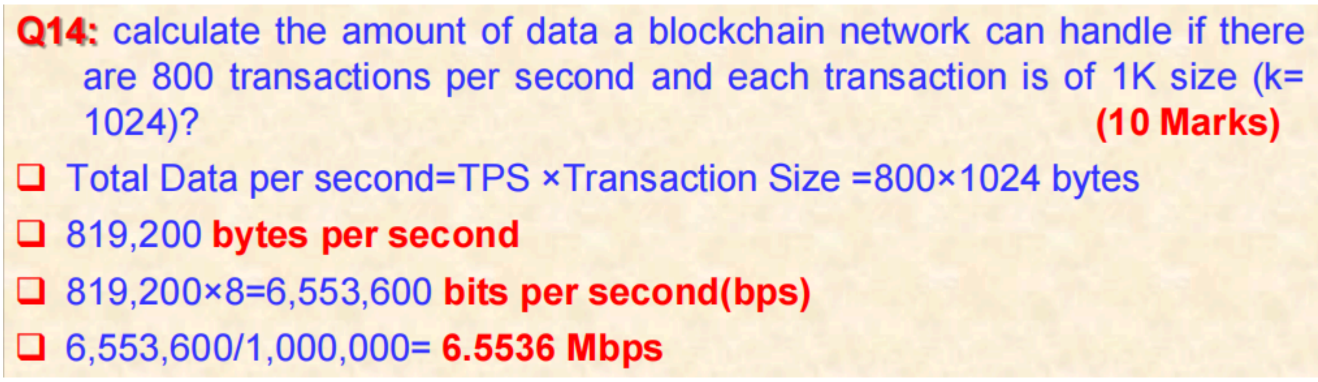
$$TPB = Blocksize(bytes)/Averagetransactionsize(bytes)$$

（3）Total Data per Second in Bytes

$$Bytes/second = TPS * TransactionSize$$

bytes to bits：multiply by 8
kbytes to bytes：multiply by 1024
bits to Mbps：divided by 1000000

Example：



Q14: calculate the amount of data a blockchain network can handle if there are 800 transactions per second and each transaction is of 1K size (k= 1024)? **(10 Marks)**

□ Total Data per second=TPS ×Transaction Size =800×1024 bytes
□ 819,200 **bytes per second**
□ 819,200×8=6,553,600 **bits per second(bps)**
□ 6,553,600/1,000,000= **6.5536 Mbps**

4.区块链的组成部分

（1）transaction事务

描述： The record of an event, cryptographically secured with a digital signature, that is verified, ordered, and bundled together into blocks, form the transactions in the Blockchain.For example, Bitcoin transfer or asset transfer.记录事件并通过数字签名加密保

护，经过验证、排序后捆绑成区块。例如比特币转账或资产转移。

好处：

- Ensure transaction security (digital signature)确保事务安全性（数字签名）
- Transparent and traceable (public records)透明可追溯（公开记录）
- Support diversified asset or service records支持多样化资产或服务记录

（2）immutable ledger不可变账本

描述： Once a transaction is written onto the Blockchainno one can change it. The transaction is immutable. An error would be resolved with another entry.一旦交易被写入区块链，没有人可以改变它。事务是不可变的。错误将通过另一个事务解决。

好处：

- Data integrity guarantee数据完整性保障
- Prevent tampering and fraud防止篡改和欺诈
- Audit-friendly (Permanent record)审计友好（永久记录）

（3）Decentralized P2P Nodes去中心化对等节点

描述： Blockchain is a decentralized peer to peer network. Where each node has a copy of the ledger.区块链是去中心化的点对点网络，每个节点都有账本的副本。

好处：

- No single point of failure (strong anti-attack capability)无单点故障（抗攻击性强
- Enhance network stability and fault tolerance增强网络稳定性与容错性
- Reduce the risk of centralized corruption降低中心化腐败风险

（4）encryption加密

描述： Protect data using encryption technologies (such as hashing and digital signatures). Public chain data is transparent but encrypted, while private chains are accessed through permission control.使用加密技术（如哈希、数字签名）保护数据。公共链数据透明但加密，私有链通过权限控制访问。

好处：

- Data Privacy and Security (Leak Prevention)数据隐私与安全（防泄露）
- Identity verification (digital signature)身份验证（数字签名）
- Flexible permission management (private chain scenario)灵活权限管理（私有链场景）

（5）Consensus Mechanism共识机制

描述： Ensure that all nodes reach an agreement on the validity of transactions. Common mechanisms include PoW, PoS, DPoS, etc.确保所有节点对事务有效性达成一致，常见机制包括PoW、PoS、DPoS等。

好处：

- Network consistency 网络一致性
- Security and attack resistance安全性与抗攻击（如PoW需51%算力）
- Energy-saving and highly efficient节能高效（如PoS减少算力消耗）

（6）smart contracts智能合约

描述： The automatic execution program stored on the blockchain triggers operations (such as automatic transfer and contract fulfillment) based on preset conditions.存储在区

块链上的自动执行程序，根据预设条件触发操作（如自动转账、合约履行）。

好处：

- Eliminate intermediaries (reduce costs)消除中介（降低成本）
- Improve efficiency (immediate execution)提高效率（即时执行）
- Transparent and trustworthy (code public and auditable)透明可信（代码公开可审计）
- Support complex financial protocols (such as DeFi applications)支持复杂金融协议（如DeFi应用）

5.如何提供效率，透明度和信任（efficiency/transparency/trust)

（1）效率：Smart contract can reduce processing time and cost of transactions智能合约减少了处理时间和成本

（2）透明度：Using cryptography and hashing. It is a p2p digital ledger, everyone has a record. All information recorded is the history, every block edited is verified.
使用密码学和哈希。提供一个p2p的数字账本，每个人都有一个记录。所有被记录的信息都成为历史，每一个区块都已经被验证。所以他是透明的。(去中心化节点和不可变账本)

（3）信任：Everything that recorded and blockchain is accurate, so there is a trust build in due to encryption.由于加密和哈希，每个被记录的信息和区块都是准确的，所以存在信任。

6.如何提供安全性/稳定性（security/transparency/immutability）

Using cryptography and hashing. everything will be copied when joining in a blockchain. It use hashing and everything can not be edited. so it is a immutability system.
使用密码学和哈希加密。每个信息都会被复制进区块链。使用哈希加密算法，每个信息都不可被修改，所以是一个稳定的系统。

7.共识算法(consensus algorithms)

（1）Proof of Work (PoW)工作量证明：

描述： Nodes compete for the right to record transactions by calculating hash puzzles, consuming computing power to verify transactions.节点通过计算哈希难题竞争记账权，消耗算力验证事务。

优点： High security (requiring 51% computing power for attack), fully decentralized.高安全性（需51%算力攻击），完全去中心化。

缺点： Extremely high energy consumption and slow transaction speed (Bitcoin TPS≈7).能耗极高，事务速度慢（比特币TPS≈7）。

应用： Bitcoin, Litecoin比特币、莱特币

（2）Proof of Stake (PoS)权益证明

描述： Select validators based on the amount of coins held and time, and stake tokens as collateral.根据持币量和时间选择验证者，质押代币作为担保。

优点： Energy-saving, transaction speed improved (Ethereum 2.0TPS≈ 100,000).节能，事务速度提升（以太坊2.0TPS≈10万）。

缺点： The rich get richer (Matthew effect), which may lead to centralization.富者愈富（马太

效应），可能中心化。
应用： Ethereum 2.0, Cardano 以太坊2.0、Cardano

8.Energy Consumption Issues

（1）影响：PoW-based systems like Bitcoin consume significant energy,leading to a high carbon footprint.比特币等基于PoW的系统消耗大量能源，导致高碳足迹。
（2）解决方案：Transitioning to Proof-of-Stake, using renewable energy,optimizing mining hardware, and implementing off-chain solutions can address energy concerns.过渡到权益证明、使用可再生能源、优化采矿硬件和实施链下解决方案可以解决能源问题。

9.加密货币（cryptocurrencies）

（1）bitcion比特币
描述： Bitcoin is a decentralized digital currency，Primary concerns is transaction security and Double spends.The consensus mechanism is POW.比特币是一种去中心化的数字货币，主要关注的是交易安全性和双重支出。共识机制是工作量证明。
动机： Distrust of financial institutions and Transaction costs解决对金融机构的不信任问题并降低交易成本
优点：

- High decentralization and security高度去中心化与安全性
- very few稀缺性
- The highest brand recognition品牌认知度最高

缺点：
- The transaction speed is slow事务速度慢
- High energy consumption高能耗
- Single function (no smart contract)功能单一（无智能合约）

（2）Ethereum以太坊
描述： A programmable blockchain platform that supports smart contracts and decentralized applications, with the consensus mechanism being proof of stake.可编程区块链平台，支持智能合约和去中心化应用，共识机制是权益证明。
优点：
- Support smart contracts and complex applications (such as DeFi, NFT)支持智能合约与复杂应用
- High developer ecosystem activity高开发者生态活跃度
- High throughput高吞吐量

缺点：
- Smart contract vulnerability risk智能合约漏洞风险
- Transaction fees soar when the network is congested网络拥堵时手续费飙升
- Some decentralization controversies (Foundations have significant influence)部分去中心化争议（基金会影响力大）

（3）Ripple瑞波币

描述： Enterprise-level cross-border payment and asset settlement tools, serving financial institutions. It has a unique consensus mechanism (no mining required), and transactions are confirmed by voting of verification nodes企业级跨境支付与资产结算工具，服务于金融机构。有独特共识机制（无需挖矿），由验证节点投票确认事务

优点：

- Extremely fast transaction speed极快事务速度
- Low handling fee低手续费
- Cooperate deeply with financial institutions与金融机构深度合作

缺点：

- Highly centralized (Ripple Company controls the majority of tokens) 高度中心化（Ripple公司控制多数代币）
- Legal risk法律风险
- Pre-mining tokens has raised questions about fairness预挖代币引发公平性质疑

DeFi（Decentralized Finance）去中心化金融

1.DeFi描述

DeFi, or Decentralized Finance, refers to a new movement within the cryptocurrency and blockchain industry that seeks to provide traditional financial services such as lending, borrowing, and trading, using decentralized protocols and applications that operate on public blockchain networks.
DeFi，即去中心化金融（Decentralized Finance），指的是加密货币和区块链行业内的一项新运动，旨在通过在公共区块链上运行的去中心化协议和应用程序，提供传统的金融服务，如贷款、借款和交易网络。

2.DeFi优缺点

（1）优点（advantages/benefits）：

Decentralization去中心化： It operates on a decentralized network, resisting censorship and single points of failure 它运行在一个去中心化的网络上, 抵制审查和单点故障
Transparency透明度：Running on the public ledger, it offers higher transparency and traceability compared to traditional finance 运行于公共账本之上,相比传统金融提供更高的透明度和可追溯性
Accessibility可及性：Provide financial services for individuals who may not have access to traditional financial services 为那些可能无法接触传统金融服务的个人提供金融服务
Lower Costs低成本： DeFi can provide financial services at a lower cost than traditional financial institutions, as they do not require intermediaries 可以以比传统金融机构更低的成本提供金融服务，因为它们不需要中介机构
Security安全性：DeFi operates on a secure blockchain network, reducing the risks of fraud and theft 去中心化金融 (DeFi) 运行于安全的区块链网络之上, 降低了欺诈与盗窃的风险

（2）缺点（disadvantages/risks）：

Volatility 波动性： Cryptocurrencies are highly volatile and can lead to sudden price drops, which could result in a loss of funds.加密货币非常不稳定，可能导致价格突然下跌，这可能导致资金损失

Security 安全性： susceptible to hacks and exploits as the platforms are not regulated由于平台不受监管，容易受到黑客攻击和利用

Complexity复杂性： for those who are not familiar with the cryptocurrency and blockchain industry 对于那些不熟悉加密货币和区块链行业的人

Immature Technology不成熟的技术: DeFi technology is immature and has yet to be fully stress-tested at scale over an extended period. Funds may be lost or put at risk.没有经过压力测试

Scaling Risk扩展风险: Current DeFi platforms use a consensus method with slow transaction speeds. Ethereum, the main technology for decentralized finance, can process 15 transactions a second, while Visa can process 65,000 a second.当前的DeFi平台使用共识方法，交易速度较慢。以太坊是去中心化金融的主要技术，每秒可以处理15笔交易，而Visa每秒可以处理65000笔交易。

为什么加密货币会波动?

There is no rules and regulations. And government do not make privacyt and framework 没有规则和规定。而政府不创造隐私和框架

3.How challenge traditional banking systems:

（1）Reducing dependency on banks and brokers.减少对银行和经纪人的依赖。

（2）Offering services with lower fees and higher accessibility.提供费用更低、可访问性更高的服务。

（3）Promoting financial inclusion for unbanked populations.DeFi's growth is pushing traditional institutions to innovate and adopt blockchain-based solutions.促进无银行账户人群的金融普惠。DeFi的增长正在推动传统机构创新并采用基于区块链的解决方案。

4.智能合约（smart contract）对DeFi应用有哪些优势/作用?

（1）**Eliminating Intermediaries无中心中介:** No reliance on third parties.

（2）**Security & Transparency安全性和透明度**: Transactions are immutable and verifiable. 交易是不可变和可验证的

（3）**Cost Efficiency成本效率:** Reduces fees by eliminating banks and brokers.通过取消银行和经纪人来降低费用

（4）**Availability可用性**: DeFi protocols operate continuously without downtime.可连续运行，无需停机

（5）**Automated Transactions自动交易**: Transactions are triggered automatically.

（6）**Interoperability互操作性**: In the DeFi space, smart contracts can interact with each other to create complex financial protocols, enabling features like automated market making, decentralized exchanges, and liquidity pools.智能合约可以相互交互，创建复杂的金融协议，实现自动做市、去中心化交易所和流动性池等功能。

Smart contracts revolutionize DeFi by automating financial services,reducing costs, and enhancing accessibility. They enable lending, trading,and investment without intermediaries, paving the way for a more inclusive and decentralized financial system.智能合约通过自动化金融服务、降低成本和提高可访问性，彻底改变了DeFi。它们使借贷、交易和投资无需中介，为一个更具包容性和去中心化的金融体系铺平了道路。

5.区块链在DeFi中的作用

DeFi is based on blockchain. It provides low cost, transparency, immutability and trust.DeFi基于区块链。它提供了低成本、透明、不变性和信任。

6.未来展望

（1）加密货币: increasing acceptance for transactions and investments but require regulatory clarity and environmental solutions.交易和投资的接受度越来越高，但需要监管清晰和环境解决方案。

（2）DeFi： DeFi has grown tremendously over the past few years, however,the future of DeFi is highly dependent on factors like including the adoption and use of blockchain technology, regulatory changes,and advancements in the ecosystem.Overall, DeFi has the potential to revolutionize the financial industry by providing greater financial access and inclusivity.

DeFi在过去几年中发展迅猛，然而，DeFi的未来高度依赖于诸如区块链技术的采用和使用、监管变化和生态系统的发展等因素。总体而言，DeFi有潜力通过提供更大的金融准入和包容性来彻底改变金融业。

（3）区块链： Broad applications across industries; expected to play a vital role in securing, streamlining, and decentralizing systems globally.跨行业的广泛应用；预计将在全球范围内保护、简化和分散系统方面发挥至关重要的作用。