CIA: a general set of properties in InfoSec.

Confidentiality: 信息具有保密性，不会被不当的人获取。

Integrity: 在生命周期内保持正确和不变。

Availability: 信息可被访问，可用性是保证的。

一些词汇：

Ransomware	勒索软件
Malware	木马（恶意软件）
Eavesdropping	窃听
Maliciously	恶意地

Spoofing	假装成其它用户 — Authenticity
Tampering	篡改数据 (altering interactions) — Integrity
Repudiation	否认做了某事 — Non-repudiability
Information Disclosure	数据泄漏 — Confidentiality
Denial of Service	使服务资源耗尽 — Availability
Elevation of Privilege	使权限提升 — Authorization

Threats: 包括上述六种在内的危险后果。(被对手如何利用)

Vulnerability: 漏洞，使上述后果发生的原因。

Likelihood: 上述问题出事的可能性。

Impact: 后果

Protection: 保护措施

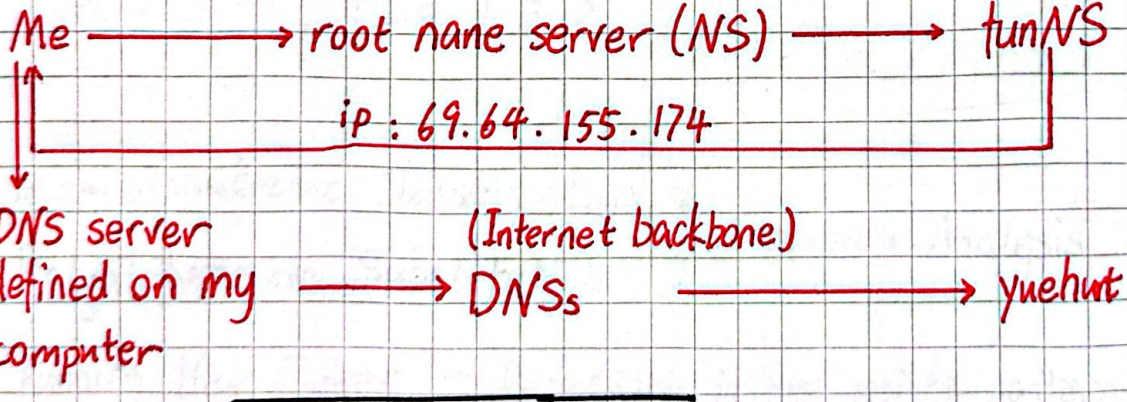
Security Principles:

1. Economy of Mechanisms : Simple
2. Least Privilege : Using necessary privileges
3. Least Common Mechanism : Less share mechanism
4. Fail-Safe Defaults : Deny access by default
5. Complete Mediation : Check all access attempts
6. Open Design : Attackers can know design.
7. Psychological Acceptability : Easy to use for human
8. Separation of Privilege : More than one key
   如核钥匙

top level domain

http:// yuehunt.fun / puzzles

- http:// : protocol specifier
- yuehunt.fun : domain name
- puzzles : page location



Packets:

一些信息(几百bit)
My IP address
yuehunt IP address
"Some message"

← 使用HTTPS可以确保其不被修改或其它人查看

辗转相除法

如 gcd(1169, 560) = ?

$1169 = 560 \times 2 + 49$

$560 = 49 \times 11 + 21$

$29 = 21 \times 2 + 7$

$21 = 7 \times 3$

欧拉函数 Euler's totient function: (这个不考)

$$\varphi(N) = |\{x \in \{1, \cdots, N-1\} \mid \gcd(x, N) = 1\}|$$

欧拉定理指出，对任意 $x \in (\mathbb{Z}/N\mathbb{Z})^*$ 有

$$x^{\varphi(N)} \equiv 1 \pmod{N}$$

例如对 $N=10$，有 1, 3, 7, 9 与其互质，故 $\varphi(N) = 4$。

可以求得 $1^4 = 1$，$3^4 = 81 = 1$，$7^4 = 2401 = 1$，$9^4 = 6561 = 1$

如此，对于求 7^{2023} 的个位之类的问题，我们易得 $2023 = 4 \times 505 + 3$

即 $7^{2020} = 1$，答案是 $7^3 = 3$

Monoalphabetic Substitution
Polyalphabetic Substitution
→ Frequency Analysis

Running Key Cipher → Repetition in key yeilds patterns.

指定了一本字典中的段落进行移表加密，需要尽可能长的段落防止被攻破。

One-Time pad 密码需求量很大。

Symmetric Key Encryption

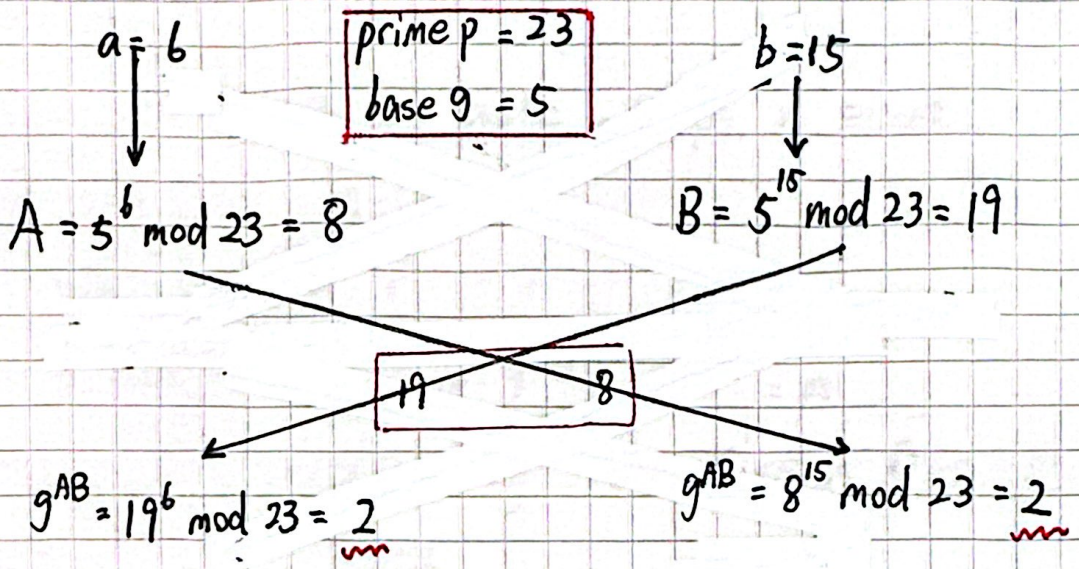
Cryptographer : person who makes the cryptography.

Cryptanalyst : person who breaks the cryptography.

Code : semantic translation (A means B)

Ciphertext : encryption of underlying plaintext

Diffie-Hellman Key Exchange (对称)



Public Key Encryption = Asymmetric Cryptography

prime p, q

$n = pq$

encryption exponent: e s.t. $\gcd(e, (p-1)(q-1)) = 1$ — makes n, e public

decryption exponent: d s.t. $de = 1 \pmod{(p-1)(q-1)}$

send $c = m^e \pmod n$ ⟶ decrypt $m = c^d \pmod n$

RSA Cryptosystem

例: $n = 91$, $e = 35$, $p = 13$, $q = 7$, $d = 35$

Hardness.

因为密码学很大，这里抽个例子写一下，考试不会算了。（听说不考数学，反正我信了）

Decisional Diffie-Hellman problem (DDH): Given g, g^x, g^y g^z, decide if $g^z = g^{xy}$ or g^r for some random $r \in \mathbb{Z}/q\mathbb{Z}$

ElGamal Encryption:

1. Choose $\langle g \rangle = C_q$ (循环群), $x \in \{1, \cdots, q-1\}$
2. $h = g^x$
3. makes ($\langle g \rangle$, q, g, h) public, keeps x secret.
4. choose $y \in \{1, \cdots, q-1\}$
5. send g^y and $m \cdot h^y$
6. $m = (m \cdot h^y) \cdot (g^y)^{-x} = m \cdot g^{xy} \cdot g^{-xy} = m$

IND-CPA (Indistinguishability (不可区分性) from Chosen Plaintext Attack):

Adversary who can pick an arbitrary plaintext m should not be able to distinguish the encryption of it from the encryption of a random message.

求证若DDH问题困难，则ElGamal encryption is IND-CPA secure.

It's hard to distinguish $h^y = g^{xy}$ from random DDH.

Thus it's hard to distinguish $m \cdot h^y$ from random.

Positive/ Negative Indicators

↑ 一般是一把锁 🔒　　↖ Chrome上是 ⓘ不安全 ~~https~~

由上面介绍的加密算法，https是重要的安全保障协议。如何提醒用户这种协议未能实现也成为了现在的浏览器的重要工作。

⚠忘说了，从数论开始到现在这章叫 Confidentiality - 保密性。这是CIA之一。

下一章叫 Integrity - 正确性。是CIA之二。

Man-in-the-Middle (MitM) Attack

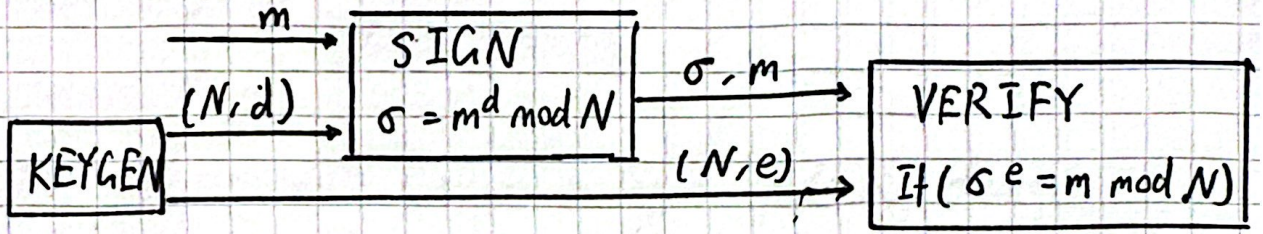
例如 Diffie-Hellman Key Exchange

中间人决定数字C

$(g^a)^a$ —$A=g^a$→ $(g^a)^c$ ←$C=g^c$— $(g^c)^b$　　$(g^b)^c$ —$B=g^b$→ $(g^c)^b$ ←$C=g^c$—

Digital Signatures

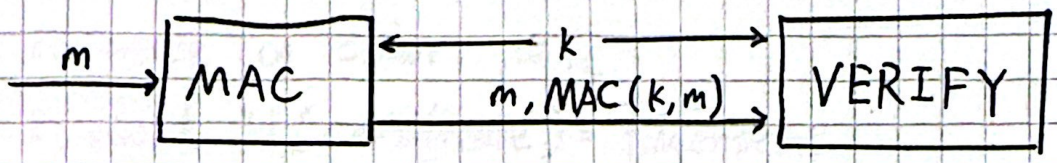
若用 Textbook RSA



但其不能防止 adversary gets signatures：

若有 σ_1, σ_2 由 m_1, m_2 生成 $\sigma = \sigma_1 \cdot \sigma_2$ 可与 $m_1 \cdot m_2$ 通过验证。

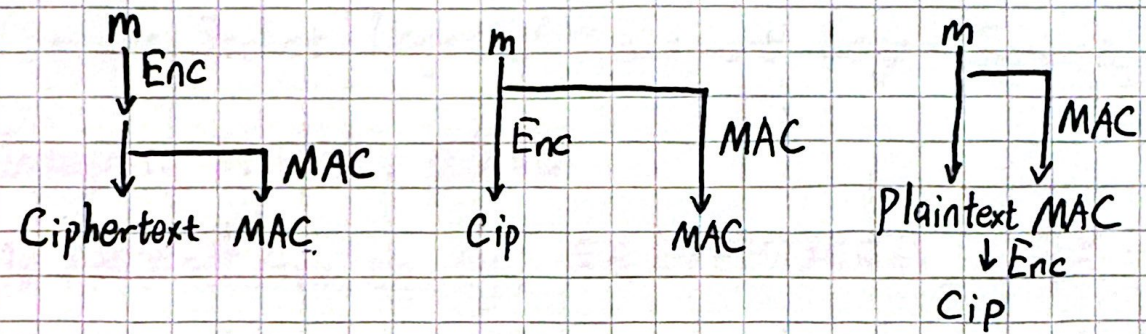
Message Authentication Codes (MACs)



Correctness: Verify(k, m, MAC(k,m)) = 1

Unforgeability: Hard to generate MAC(k,m) without knowing k.

Authenticated Encryption (认证加密) with Associated Data (AEAD)



Hash Function:

$H: \{0,1\}^* \rightarrow \{0,1\}^k$ ← 算法规定的特定长度

↑ 任意长度

uniformity: even small changes in input yield big changes in output

uniqueness: There is low chance of collision

1. Pre-image resistance
   $H(x) \rightarrow x$ is hard
2. Collision resistance
   $H(x) = H(y)$ is hard

Applications: File Checksum, MACs, Digital Signatures, Commitments, Blockchains, Virus scanning, Password storage.

Digital Certificates

SSL / TLS Handshake

1. agree on cipher suite
2. check $H(\text{certificate}) = \text{fingerprint}$
   check $\text{Verify}(PK_{CA}, sig, pk_{service})$
3. client sends $c = \text{Enc}(pk_{service}, sk)$
   service uses $sk = \text{Dec}(sk_{service}, c)$
4. use sk to do AEAD.
5. Terminate connection

Secure Socket Layer / Transport Layer Security

Integrity 到此结束。

接下来要讲 Availability，其是三个部分构成的，分别是：

Hardware failures, Malware, 和 Denial of Service (DoS)

其中第一点非常无聊，我们的介绍从 DoS 开始。

Amplification:

Use small number of packets ⇒ obtain a big effect

① DoS bug: Design flaw (缺陷) allowing one machine to disrupt a service.

② DoS flood: Command botnet to generate flood of requests.

对抗的方法有：

① Client Puzzles 让每个客户端在被攻击期间做题加大攻击者消耗

现代的题目一般考验内存而非CPU，因为手机算力不行但内存差不多。

② CAPTCHAs

~~确认你是人类~~

③ Source Identification

从根源上解决问题。

(a) 检查信源IP (Ingress Filtering)

问题：要求所有ISP(服务商)仅转发具有合法IP(legitimate source IP)的信息，否则完全无效。

(b) 回溯 (Traceback)

检查回到信源的路径。

也要求节点将自己的IP写入packet

这可能导致packet过大，故可以要求节点概率性写入自身数据。

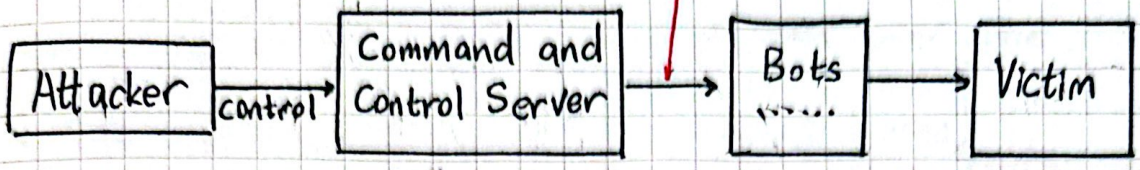
因为DDoS的规模一定很大，故可以有效还原。

但总之……

Current Internet is ill-equipped to handle DDoS attacks.

Bot (zombie) is a compromised machine that can be controlled by an attacker remotely.

update, download file at an url, run a shell command .....



Could be multiple layers of hosts between bot and botmaster.

push: command → response

pull: periodically ask → command

Peer-to-Peer C&C

More difficult to catch botmaster

Keep activities even if some nodes are down.

Bullet-Proof Hosting:

Some C&C is hosted by ISPs that are completely unresponsive to abuse complaints.

De-peering involves law enforcement.

Malware: (Malicious Code)

characteristic: perform some unwanted activity.

virus ∈ malware but not exactly same.

Virus: A program that can infect (感染) other programs by modifying them to include a version of itself.

防御: ① Signature-based detection (like hash)
② Heuristics (check for signs of infection)
③ Behavioral signature (密码的迈克菲删我C代码)
④ Sandboxing: run in restricted environment.

] Antivirus software

Worms: Autonomous spread over network
Self-contained (区别于病毒要植入进其他文件)
Speed of spreading may increase over time.

防御: ① Virus scanners (email-based worms)

Host-level:
② ASLR (address space layout randomization) Attempts to achieve diversity to increase protection.
③ Not effective when users execute malware themselves.

Network level:
④ Personal firewall
⑤ Limit the number of outgoing connections.

Trojan Horses (TH): Require the user to explicitly (显式) run the programme.
不可复制.

有2种可能: ①伪装成游戏, 屏保, 甚至compiler
②伪装成文件

防御: 不要无视④风险

Spyware: Leak sensitive information.

Keyloggers: Record key strokes typed by user.

non-spreading
self-contained

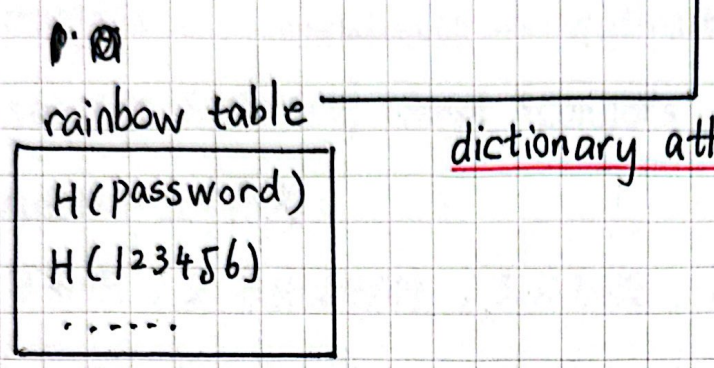
Rootkits: Enable continued privilege of a malicious program.
↑non-spreading, need host program

Authentication

密码的章节，你输入了密码

uname, passwd → 计 H(passwd) == .....

one-way function



现在电脑(25核+GPU)的尝试次数是每秒3千亿(300 billion)次。

可以在服务器存 S, h(passwd||s)

相对不容易被直接移库。 ↑连字

Salting

6salt$hash

↑ ↑一个在第一次设置密码时随机指定的数字

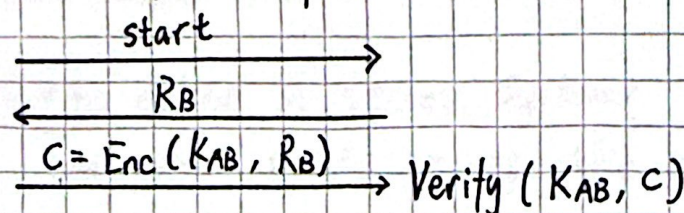
SHA-512

这样就防止彩虹表攻击

用户要做到：

1. Unaided recall (无记忆辅助)
2. Recall & entry 100% correct
3. No corrective feedback on failure (如用户名不存在)
4. No re-use.
5. No writing down.
6. No relying on reset.

Challenge Response



Biometrics : enrolment → authentication

fingerprint scanners, hand scanners, retina (视网膜) scanners.

要考虑以下四个维度：

1. 可用性，2. 易维护性，3. 识别度，4. 特征维持性

ad. nothing to remember

can't share

disad. Not secret (on glass, say)

False match in large amoung of people.

Multi-Factor Authentication

Security Key > On-device prompt > SMS code

Phishing - email

Vishing - phone call

Smishing - SMS

} 电信诈骗

Access Control

How to define a secure System?

one that meets a specific security policy.

How to define a security policy?

use threat model and build policy to address it.

Access control is the ability of one entity to permit or deny the use of a particular resource to another.

Subject: An entity that is capable of accessing objects.
Including: owner, group, world.

Object: Resources.

Access Right: Including: read, write, execute, etc.

Mandatory Access Control (MAC)

User have to prove a need for information before gaining access.

Administor assigns each subject and object a set of attributes (privilege).

Discretionary Access Control (DAC)

Owner (not administrator) can grants access to others.

1. not exceed their own 2. no contradiction with admin.

Role Based Access Control (RBAC)

根据 Least Privilege principle.

请回到正文第二页熟记7个principles. 本章节结束。

Security in *

(A) Software

~ Vulnerability : a bug that allows a user capabilities that should be denied to them.

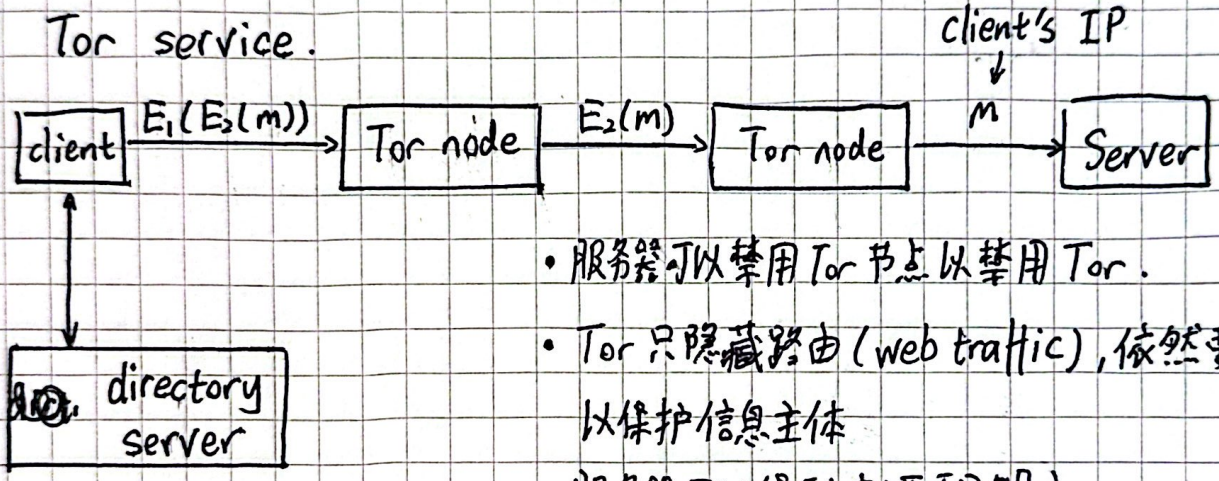
例子：Butter overflows : Happen when a program writes data beyond its allocated buffers.

(B) Web

基本写在正文第2页下方。

(C) For Sequrity to Anonymity (匿名)

Tor service.



- 服务器可以禁用Tor节点以禁用Tor.
- Tor只隐藏路由(web traffic),依然要HTTPS以保护信息主体
- 服务器可以得到来源IP明文.

(D) Attact on Integrity (CIA之正确性)

SQL injection : execute SQL command.

clickjacking : Use fake cursor(光标) or button to cover the real one.

XSS/CSRF : Cross Site Scripting:

使用JavaScript劫持身份或偷取Cookie.

Cross-Site Request Forgery:

在登录网站(如银行)的情况下,使用Cookie向其发送转账请求。

XSS: injection attack on web pages. The malicious script can access any cookies, session tokens.
Blocklisting — Allowlisting
exploits the client's trust of the server.

CSRF: Exploits the servers trust of the client.

CSRF token; string tied to a user's session but not submitted automatically.