ELEC-4120 Tutorial 10
Network Security - 2

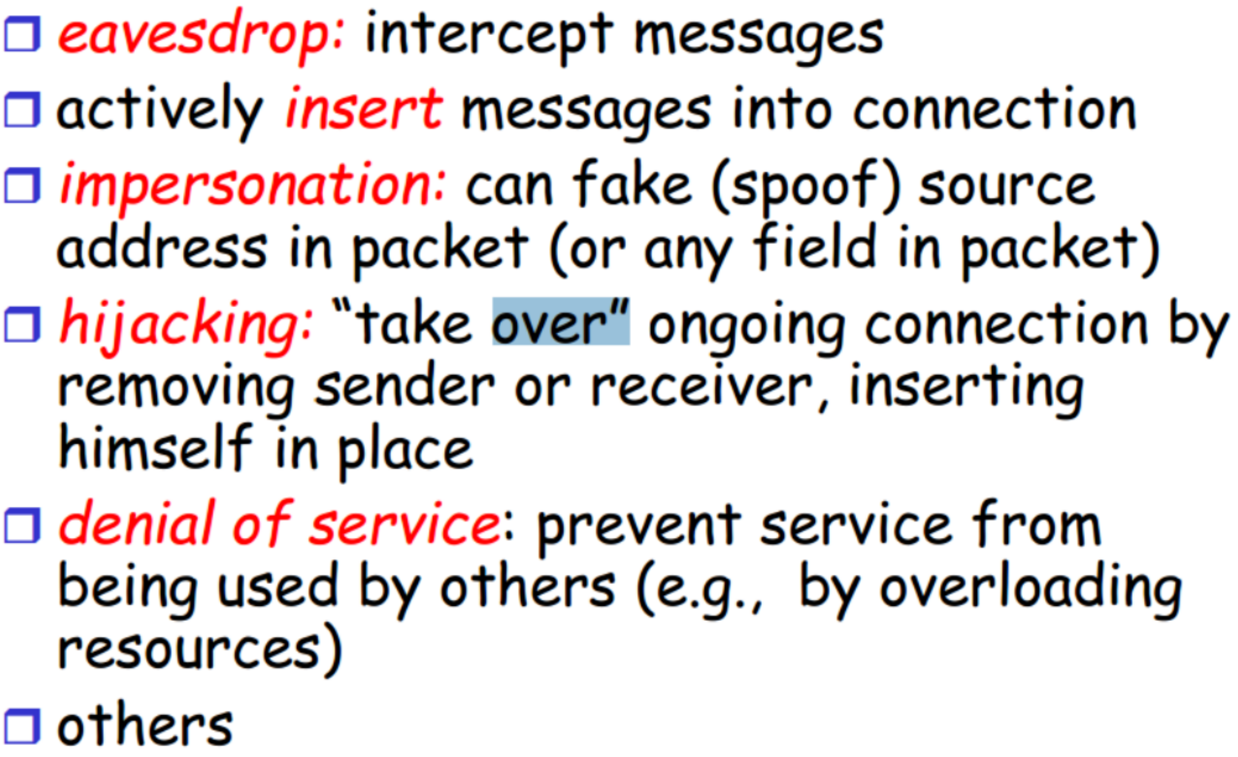
Manohar Kuse
mpkuse@ust.hk
http://ihome.ust.hk/~mpkuse

Review from previous tutorial

Review from last tutorial

- Attacks
- Symmetric Key cryptography
- Public Key cryptography & RSA Algorithm

Attacks



- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)
- others

Symmetric Key Cryptography

Password to Encrypt

&

Password to decrypt

are the **same**

What is a ‘Public key’ & ‘Private key’

Each person has 2 set of keys

-1- Public key → Tell this key to everyone

-2- Private key → Only you know this key

RSA Algorithm

There are 2 keys (K1, K2)

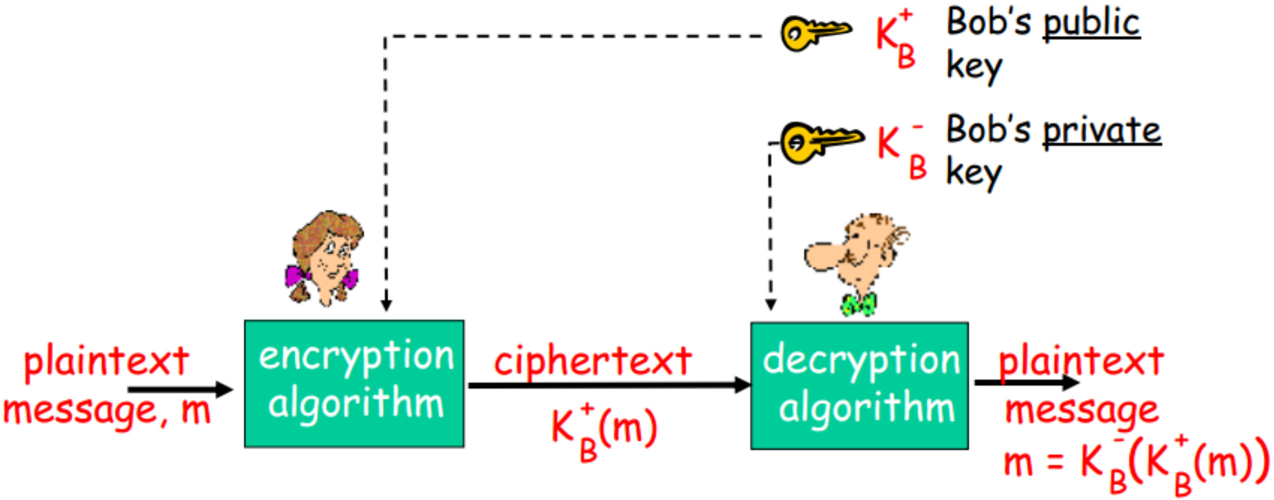
plaintext $\xrightarrow{K1}$ encrypted message $\xrightarrow{K2}$ plaintext

OR

plaintext $\xrightarrow{K2}$ encrypted message $\xrightarrow{K1}$ plaintext

How to perform RSA calculations : http://sergematovic.tripod.com/rsa1.html

How all this plays together?



Authentication

What is Authentication?

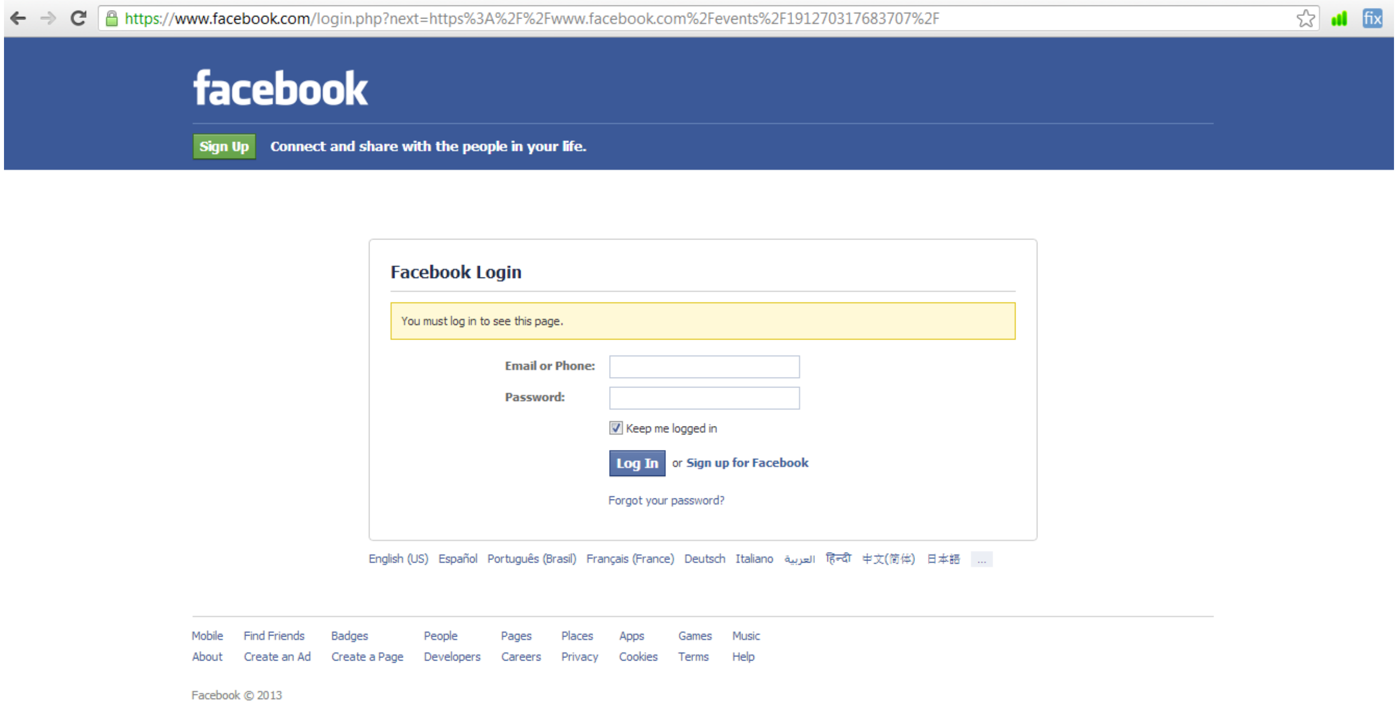
Authentication is the process of verifying that

"you are who you say you are"

Typical applications include :

After verifying your identity (for example, with password) display for you the information as per your access rights

Authentication in Use



https://www.facebook.com/login.php?next=https%3A%2F%2Fwww.facebook.com%2Fevents%2F191270317683707%2F

facebook

Sign Up Connect and share with the people in your life.

Facebook Login

You must log in to see this page.

Email or Phone:

Password:

☑ Keep me logged in

Log In or Sign up for Facebook

Forgot your password?

English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) 日本語 ...

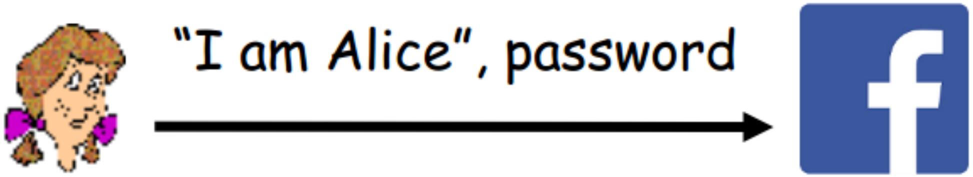
Mobile Find Friends Badges People Pages Places Apps Games Music
About Create an Ad Create a Page Developers Careers Privacy Cookies Terms Help

Facebook © 2013

Method - 1 (Simple)

User Name: alice

Password: alice2000



“I am Alice”, password

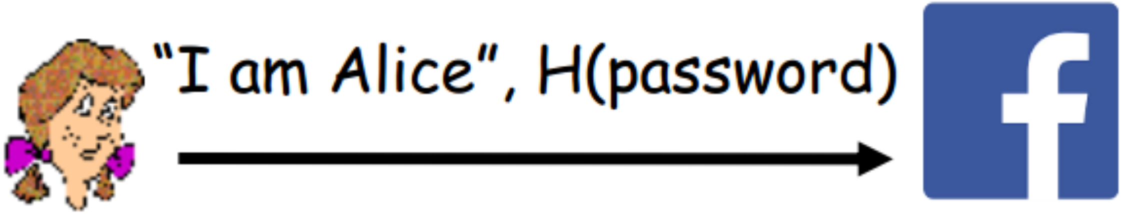
server : the password file is usually hashed

The obvious flaw of this method is that everyone can see Alice's password.

Method - 2 (Hashed Password)

User Name: alice

Password: H(alice2100)

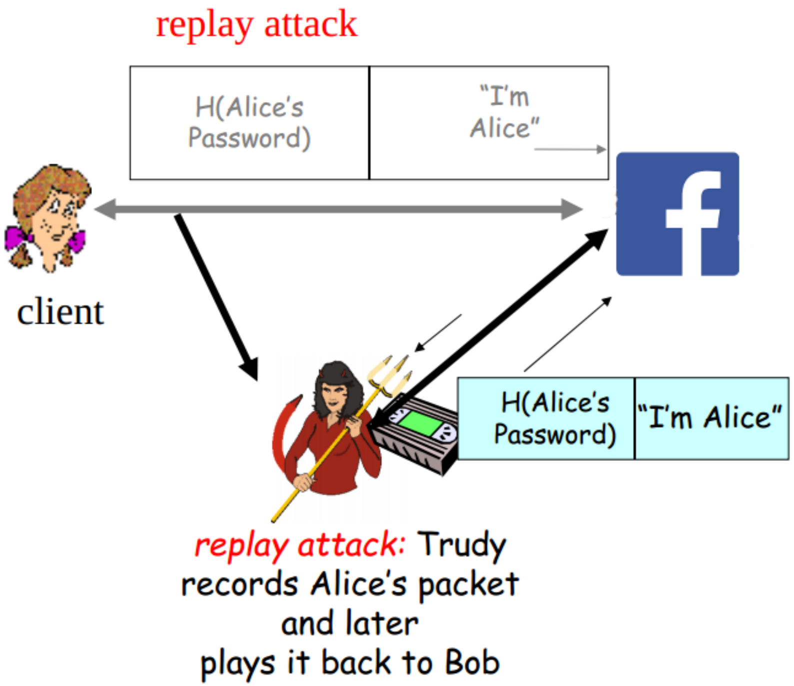


"I am Alice", H(password)

server : the password file is usually hashed

More on cryptographic hash functions : http://en.wikipedia.org/wiki/Cryptographic_hash_function
Hash function in use on internet : MD5, SHA-3

Replay can break method-2



replay attack: Trudy records Alice's packet and later plays it back to Bob

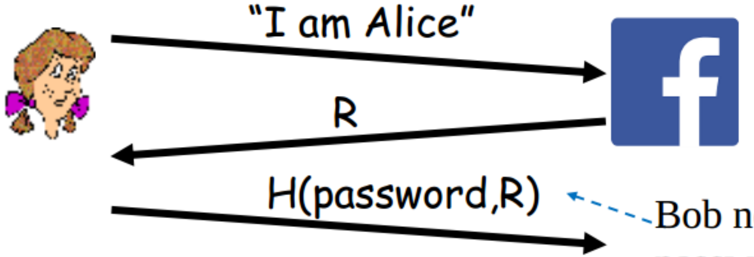
*Another name for "replay attack" is "man in the middle attack"

Method - 3

Initially don’t send the password

Server responds a random number ‘R’

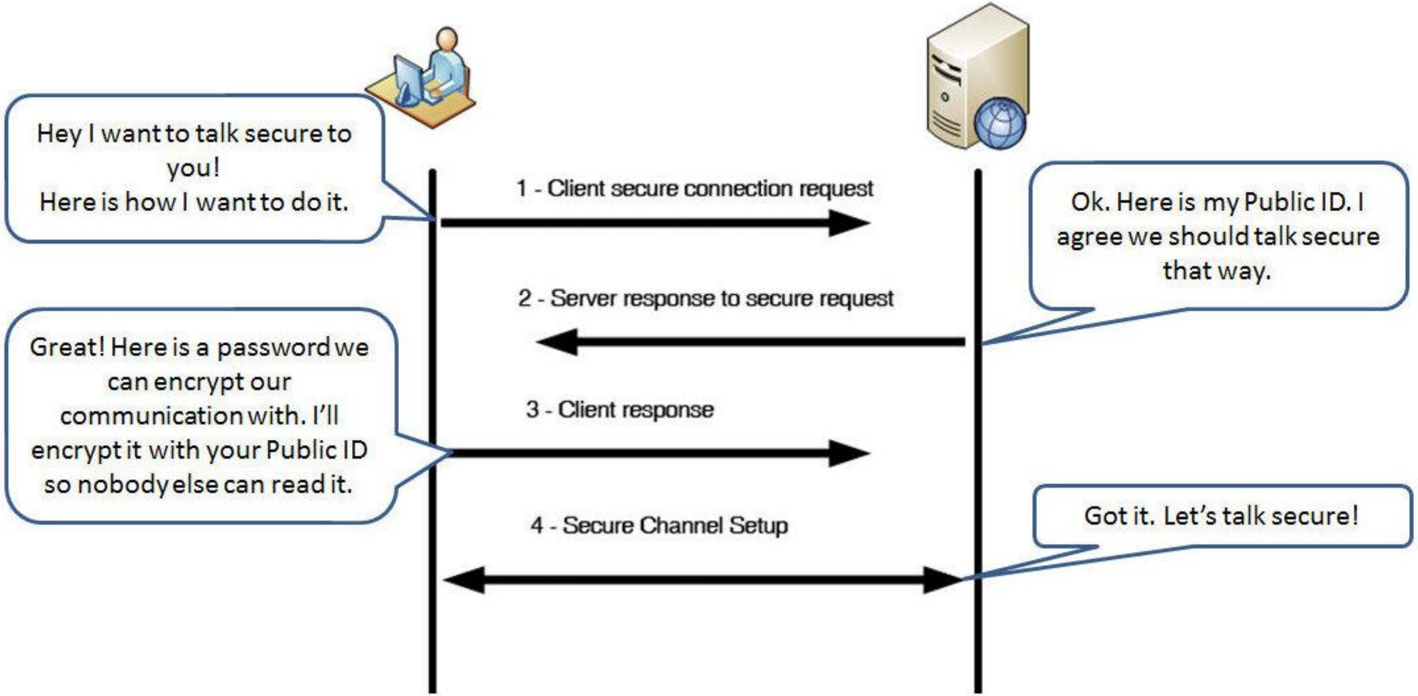
Client responds back with hash of “passwor



Bob needs to know the passwords

Real World Authentication
(Basics of SSL)

Real World Secure Communication



Hey I want to talk secure to you!
Here is how I want to do it.

1 - Client secure connection request

Ok. Here is my Public ID. I agree we should talk secure that way.

2 - Server response to secure request

Great! Here is a password we can encrypt our communication with. I'll encrypt it with your Public ID so nobody else can read it.

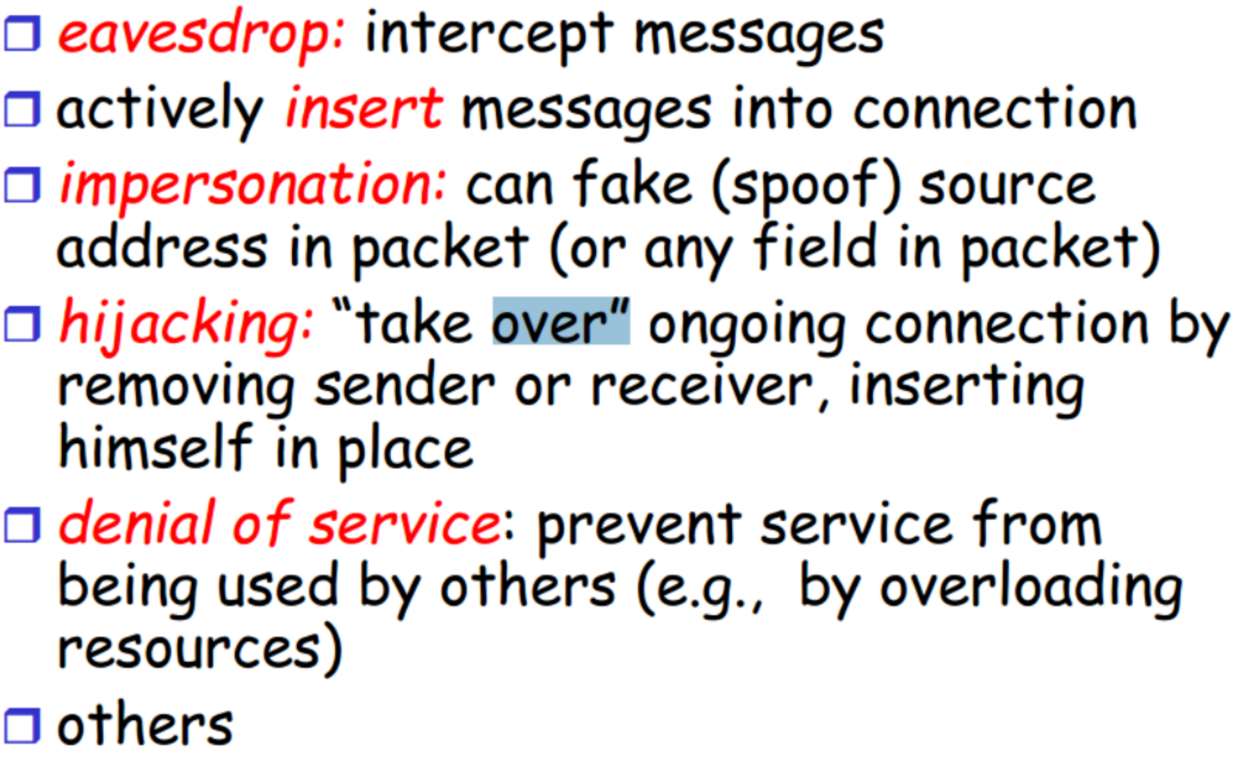
3 - Client response

4 - Secure Channel Setup

Got it. Let's talk secure!

Note: This scheme is currently in use on internet. It is called SSL (Secure Socket Layer). When you browse sites which say "https" this is exactly what is going on.

Analyze this Scheme...



- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)
- others

How to Authenticate?

1. Establish a secure communication link (see figure)
2. Server asks for username & password
3. Client Responds back with it encrypted with the agreed symmetric key

```
    if( username,password match )
        server gives away the info
    else
        bbye client…!
```

SSL in Use

Secure web browsing - HTTPS

Instant Messaging

VoIP (Voice over internet protocol) - Skype

More Info : http://en.wikipedia.org/wiki/Secure_Sockets_Layer

OpenSSL - Programming Library

Use OpenSSL library to have encryption functionality in your own softwares

http://en.wikipedia.org/wiki/OpenSSL

https://www.openssl.org/

Capabilities :

Ciphers

AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, Triple DES, GOST 28147-89[6]

Cryptographic hash functions

MD5, MD4, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, GOST R 34.11-94[6]

Public-key cryptography

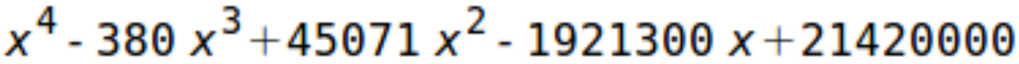
RSA, DSA, Diffie–Hellman key exchange, Elliptic curve, GOST R 34.10-2001[6]

Some Brain Teasers - Demo

Problem - 1

Tough math problem -

Find roots of this equation



$$x^4 - 380\,x^3 + 45071\,x^2 - 1921300\,x + 21420000$$

10:00 : Problem proposed to Mr. Chan & Dr. Lee

11:00 : Mr. Chan claims, “I know the answer”

11:30 : Dr. Lee says, “I bet that you being a non PhD cannot solve this problem. You send me your solution now. We meet later in the evening, if I cannot solve this problem I pay you $100.”

Security aspect : Dr. Lee may look at the answer sent by Mr. Chan and claim it as his answer. How do we safegaurd against this without using encryption?

Solution :

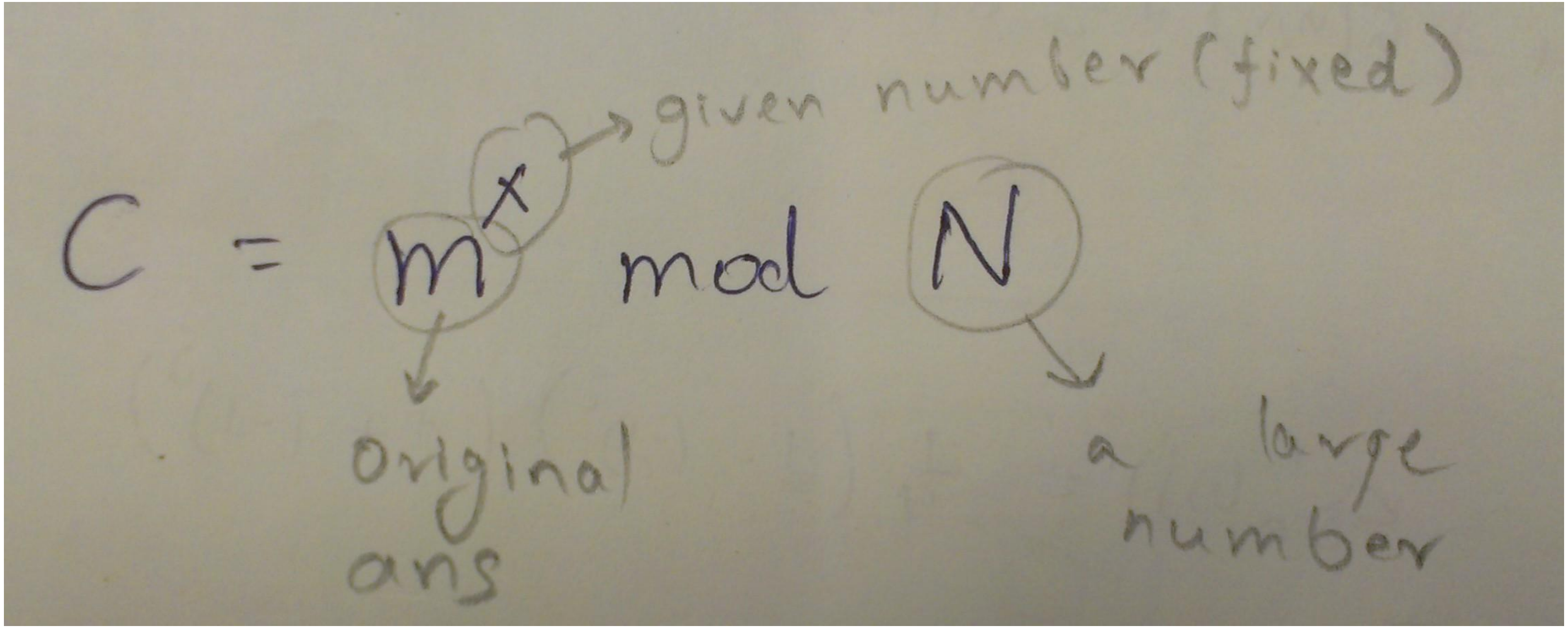
Mr. Chan should use a simple hashing scheme

Send to Dr. Lee “Ans mod 7” and not the actual answers. Ofcourse don’t tell this scheme to Dr. Lee.

200, 100, 63, 17 ⇒ 4, 2, 0, 3

Note : with (4,2,0,3) its almost impossible for Dr. Lee to come up with the solution to the problem. But Mr. Chan can immediate prove that 4,2,0,3 has come from his solution

General Hashing Scheme - Simple



$$C = m^{x} \bmod N$$

given number (fixed)

original ans

a large number