COMPUTER PRINCIPLES FOR PROGRAMMERS

Secure Computing:

Passwords, PINs, Problems, and Privacy.

Credentials > Authentication > Authorization

News of the Week

- https://www.youtube.com/watch?v=juQcZO_WnsI
  - NEWS TO SET UP LECTURE, from 2011 but still current.

Challenges in Secure Computing

- Lecture:
  1. Credentials, Authentication, Authorization
  2. Secure computing and networking
  3. Passwords, PINs, and problems

- Activity: Security and Privacy

  What are you going to do about your passwords?

  Are Facebook, Google, SnapChat, InstaGram, and a host of others, really *free*?

What is the Price of Free?

**If you don't buy the product,
you *are* the product.**

- Are free sites really free?
- Who owns the content?
- Is the benefit worth the bargain?

Credentials

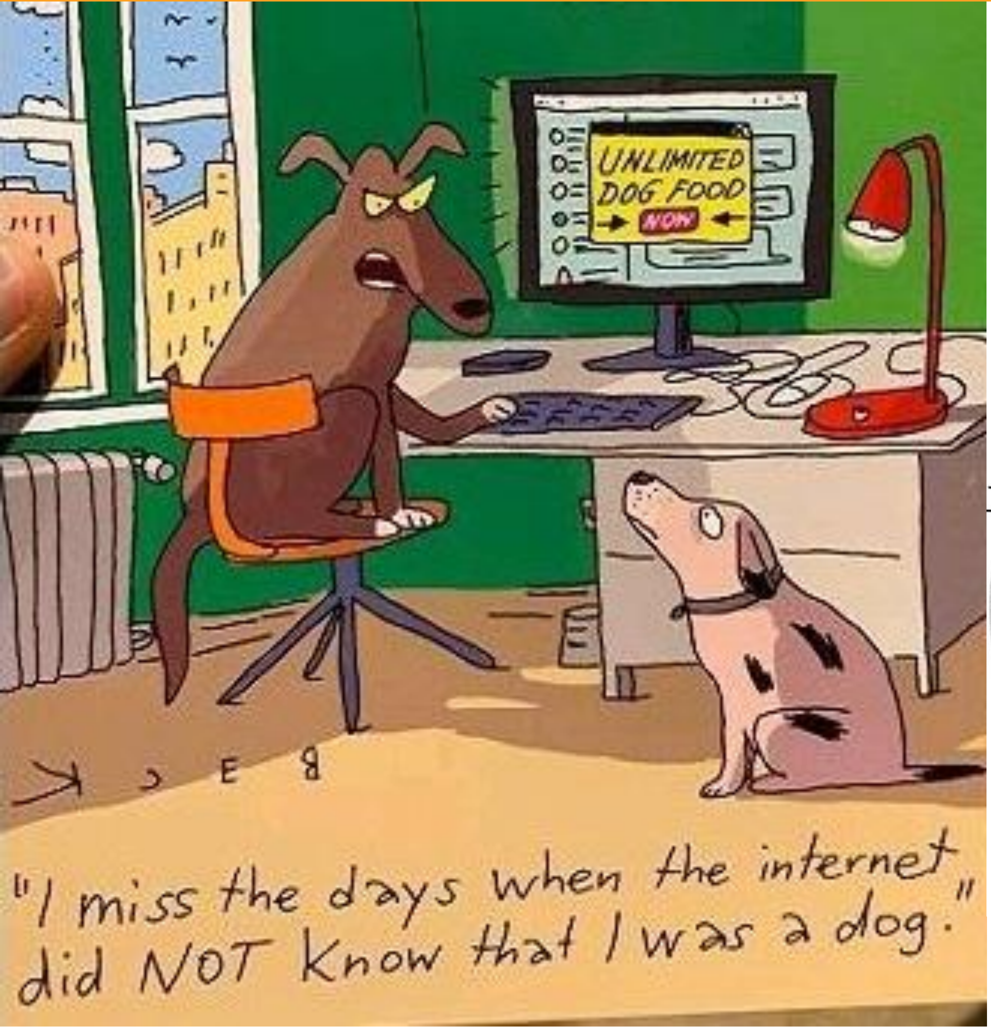
"On the Internet, nobody knows you're a dog."

Peter Steiner

The New Yorker

July 5, 1993

"On the Internet, nobody knows you're a dog."



"I miss the days when the internet did NOT Know that I was a dog."

"On Twitter, nobody verifies you're a dog."

Credentials and Authentication

Credentials:

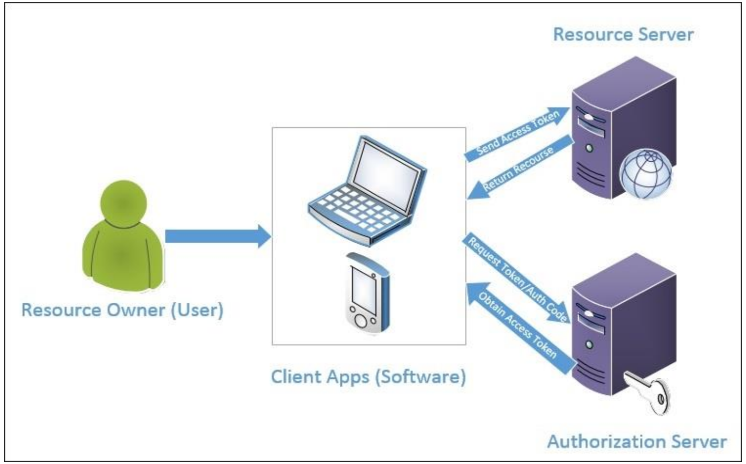
- **Identification**
- **Association**

Authentication:

- **Verifying the identity implies valid association**

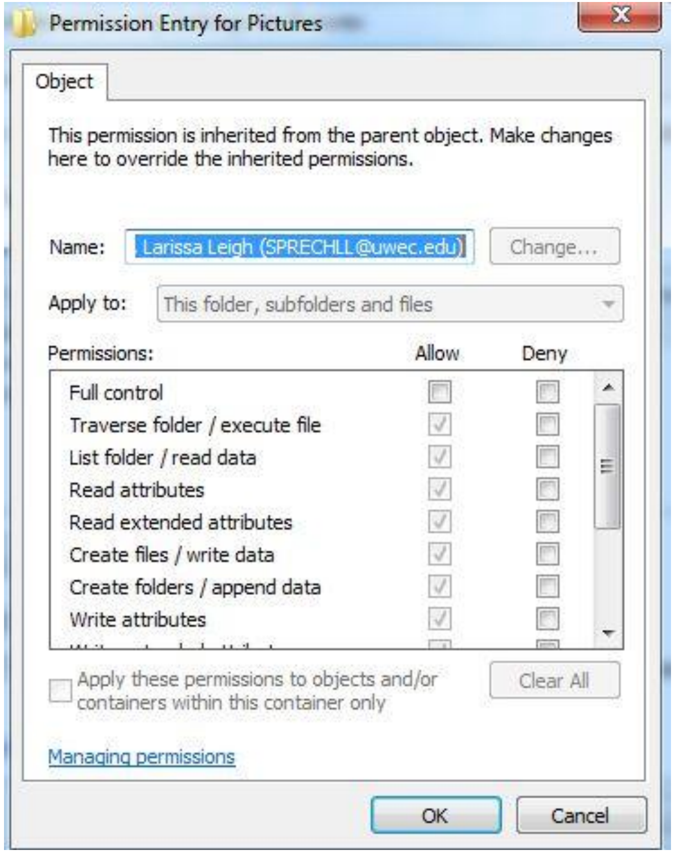
Authorization after Authentication

- Authorization is “giving someone permission to do or to access something.” e.g. access to a system/network, a directory/folder, to read and/or write a file.
- **“least privilege” principle: grant only the minimum authority needed**
- Where high level authority is needed, e.g. to reset a password, wrap it inside a program/script which inherits the needed authority but restricts action and effects.
- **What about you and other IT people?**
  You need authority to everything…*rarely*.
- **Minimum THREE UserIDs:**
- one for development system (all authorities)
- one for production server (read only authority)
- one used *only* for admin and security
  - be SuperUser (sudo) or root only when necessary
    – mistakes can be fatal to your career and company



What is “Authorization”?

- Permission = access rights = Authorization
- *unix > chmod (change mode)
  - Permissions: read, write, execute
  - Classes: user, group, others
  - Security-Enhanced Linux
- OS security controls what users can view, change, navigate, or execute



Permission Entry for Pictures

This permission is inherited from the parent object. Make changes here to override the inherited permissions.

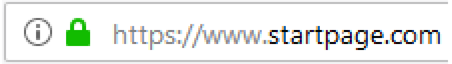
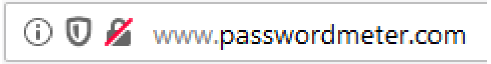
Name: Larissa Leigh (SPRECHLL@uwec.edu)

Apply to: This folder, subfolders and files

Permissions:	Allow	Deny
Full control	□	□
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	☑	□
Create folders / append data	☑	□
Write attributes	☑	□

□ Apply these permissions to objects and/or containers within this container only

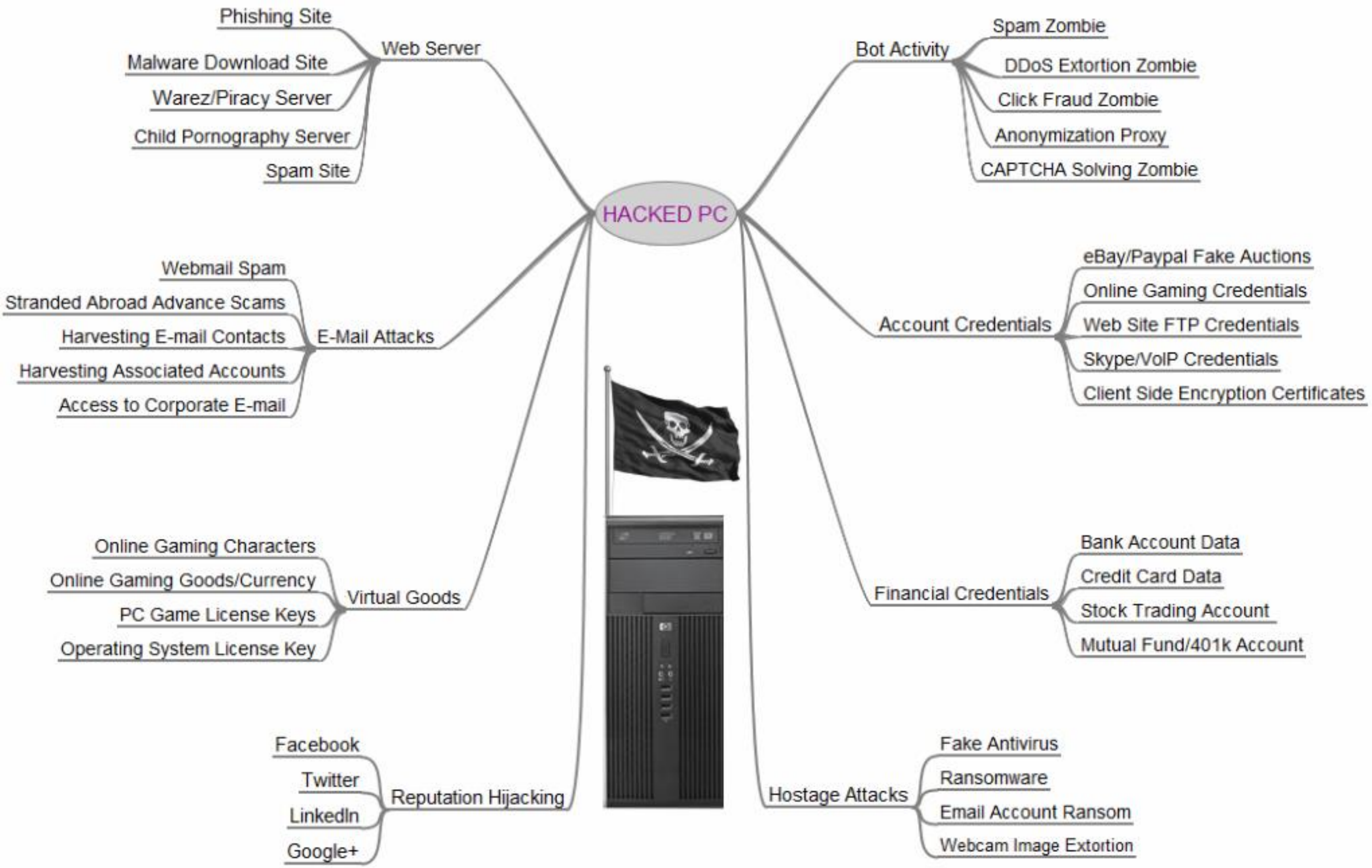
Browser Security

- HTTPS needed for sign on  https://www.startpage.com  www.passwordmeter.com
- Domain Validation (DV) certificate. Is it what you expect?
  - logitech.com rnicrosoft.com G00GLE.com Domain Checker
- DNS privacy, security, block malware, botnets, malicious domains
  - CIRA Canadian Shield Quad9 CISCO OpenDNS Cloudflare 1.1.1.1
- EFF's Privacy Badger blocks invisible trackers
- EFF's Panopticlick online tracking test
- see Increase Your Privacy Online and this and test browser

What's the password?

- Marx Brothers - Password Scene
  - Horse Feathers - Chico and Groucho
  https://www.youtube.com/watch?v=p0Gwe5gKgjo

- Who *loves* passwords?
- What if someone else knows your password?



HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

#1 most common cracking method

- **Weak Passwords**
  - guessable or reused across sites
  - **password is weak if it's not unique**
  - Top 200 Most Common Passwords
  - 25 passwords used in 10% accounts
  - 10,000 passwords used by 30% users
  - Credential Stuffing and Cracking

Forget / Recover your password

- “I forgot my password” – relies on the strength of your email account’s security and its password
- Answer Security Questions
  - "knowledge-based authentication" easy to hack
  - Google you, social media exposure, stolen wallet | bag
- Security Questions Defence: *never tell the truth*
  - But how do you keep track of the lies? (see below)

Password Edit Rules

Enter new password: `Password!1`

- Too short; minimum 8 characters.
- Must have an UPPERCASE character.
- Must have a special character.
- Must have a number.
- Expired. Must be changed.

Password Edit Rules

Rules that are BAD rules:

Length min – max → both *too short*

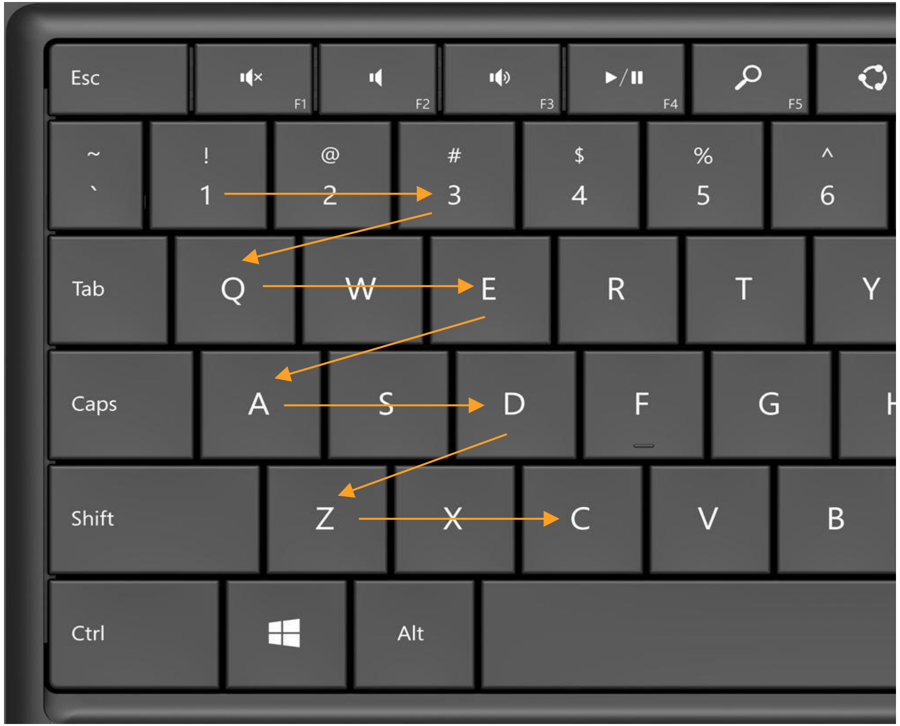
Strength alphA + digits + 5?#80!$ (symbols)
→ *too cryptic*

Not in Dictionary → *too !@#$%& cryptic*

Expiry periodic change → *too often*

Long, Strong, and INSECURE

- **13qeadzc@$WRSFXV**
- Satisfies all edit rules
- Is easy to remember
- Keyboard walk algorithm will find the pattern
- easy to remember = easy to crack



Password Defense

- Password Managers: 1Password (CDN), BitWarden (OSS), MS Authenticator (free)
  - **unique, long, random,** optionally strong passwords, per account.
  - *Must* remember one long pass-phrase.
- Diceware Pass-Phrase: long, memorable, random
  - Generate a 5 digit random number using dice. Look up the word on the list. Repeat. *Good for password managers and security questions.*
  - 1Password has a Diceware feature to satisfy bad password policies
- I have a User ID and Password!
  - End-User → sign on request → Client ← OpenID Connect → Auth. Server
  - OpenID Connect authenticates user on many sites via a single account.
  - ‘free’ OpenID service via your Google / Facebook / Twitter account. **Read the permissions requested to the authorization account!**

Password Defense

- **memorable Length instead of cryptic Strength**
  - strong is impossible to remember: `gj3ARQk+BrJe7REpL._~*0PxQ,D!Ax`
  - **Pass-*Phrase*** can be long, memorable,
    and satisfy bad rules `_Clemency0Anemone1District_...`
- Generate a long random pass-phrase. Check strength entropy
- Check if previously breached / leaked / hacked
  - https://haveibeenpwned.com/Passwords
  - https://www.passwordping.com/docs-password-strength-meter-example/
- Use an email alias for UserID
  - Firefox Relay, Mailfence (integrated with Thunderbird), Fastmail
  - Your own domain & cloud email server:
    create virtual email address for each UserID and fwd to real email mailbox

2nd most common cracking method

Social Engineering

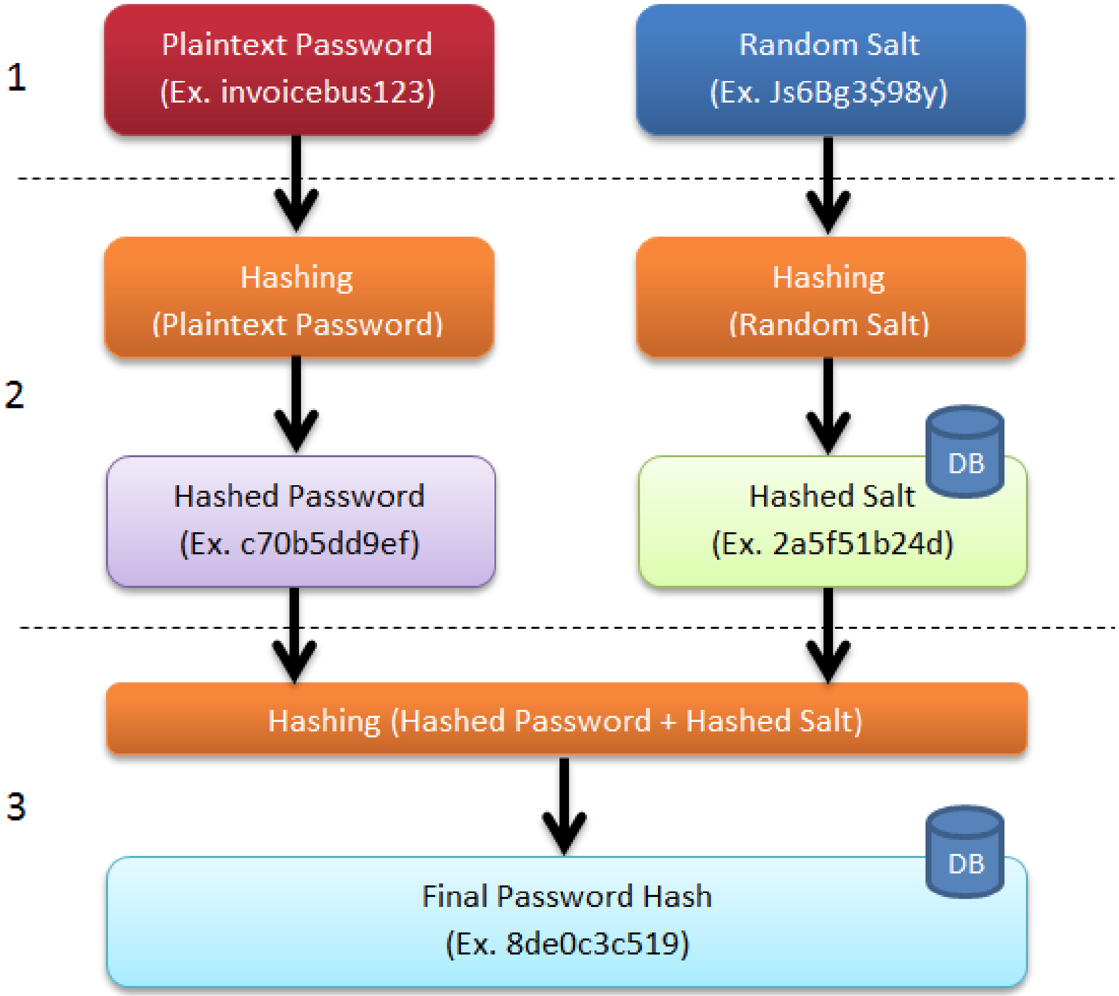
- You are your own security hole
  the more you post your life on the internet
- Spear Phishing has 35% success rate
- Social media makes it easier to guess credentials, answer security questions, pretend to be you when calling the help-desk
  or stealing your identity

Nobody can abuse information about you that they don't have.

There are two kinds of people:

1. Those who can extrapolate from incomplete data

Create User Account



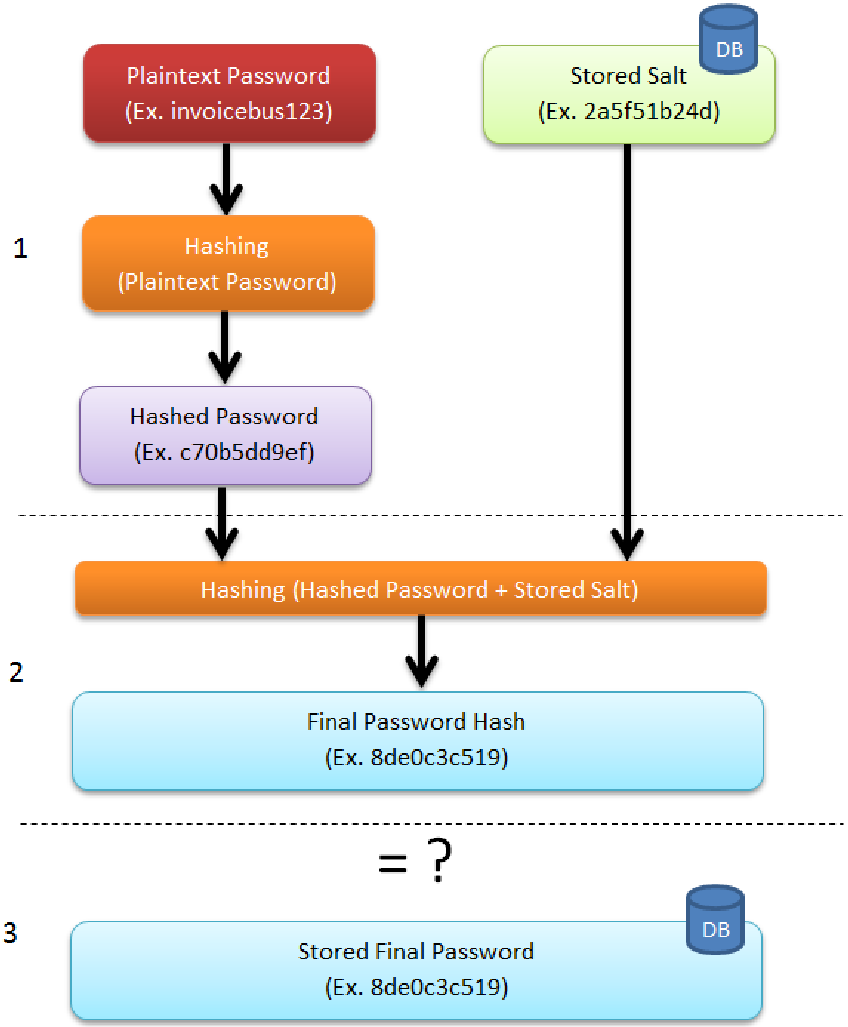
1. GET User-ID and Pwd from user input. GEN Random Salt value

2. One-way Crypto Hash of password and salt.

3a. Hash the hashes together *n* thousand times.

3b. STORE User-ID, hashed Salt, and Final Pwd+Salt Hash in DB

Authenticate User



1a. LOOKUP User-ID in DB,
GET user’s Salt-Hash.

1b. One-way Crypto Hash
of entered password.

2. Hash the hashes
n thousand times

3. COMPARE computed
Password-Salt-Hash input to
Password-Salt-Hash in DB.

Attack on whole password space of 8 letters / numbers / punctuation OR 4 random Diceware words for a single salted 100K hashed password by GPU @ 5M guesses/second: **32,500 years**

Two Factor Authentication – 2FA

- Many organizations use two factor authentication to verify password sign on and guard against phishing & cracking:

1. Something I **know**
   user ID & password, PIN
2. Something I **have**
   FIDO2 Universal 2nd Factor (U2F), phone, bank | credit | access card, YubiKey

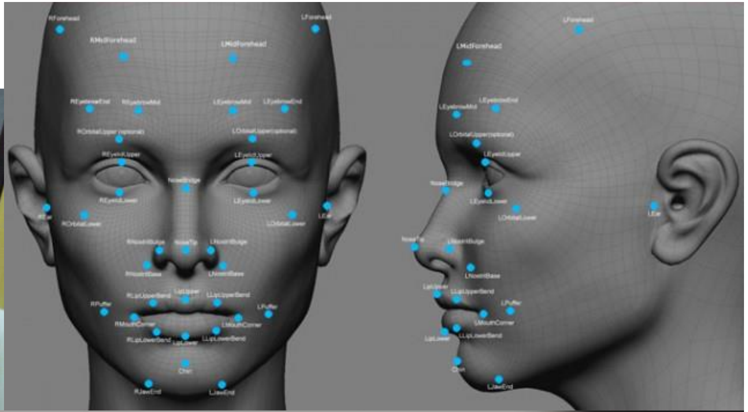
Seneca students can
add 2FA to their accounts.`

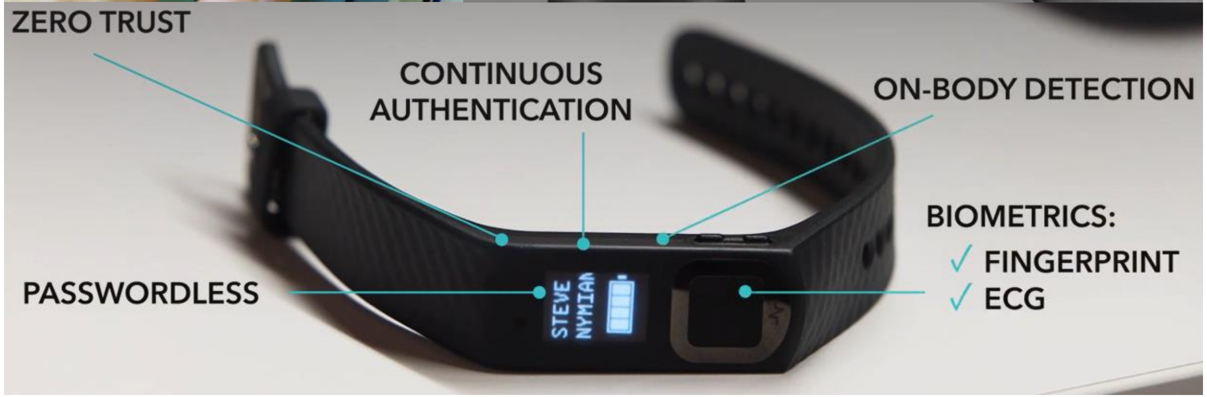
KNOWN & OWNED

Three Factor Authentication – 3FA

- Most secure and most expensive

1. Something I **know**
   user ID & password, PIN
2. Something I **have**
   smartphone, YubiKey, bank | credit | access card
3. Something I **am**
   fingerprint, facial recognition, iris scan, ECG heartbeat pattern





PIN: Probably Insecure Number

- 4 digit PINs used by banks and credit cards as 2FA
  - Ten thousand possibilities, right?
- Most people use a date to make it memorable.
- 12 mos * 31 days = 372
- 13 – 31 days * 12 mos = 228
- 1924 – 2023 years[*] = 100
- Total = **700 PINS or 7% of the range**

[*] 2001 – 2023 years already included in day/month combos

Better Password Policies

- User ID: not email address or user's name
- Pass-*Phrase* is ~~8~~ ~~10~~ ~~12~~ 14 – 64 characters in length
- No complexity rules: allow all characters including space
- Password expiration: based on risk, not time. Cannot reuse.
- Block simple dictionary, commonly used, previously breached
  - *NOT* common topology, a keyboard pattern, Pi *π*, NCC-1701-*x*
  - IT experts name Mb2.r5oHf-0t as world's safest password. (kidding)
- Require two-factor ID, e.g. Microsoft Authenticator, U2F
- Digital Identity Guidelines, NIST SP 800-63B Appendix A p.67

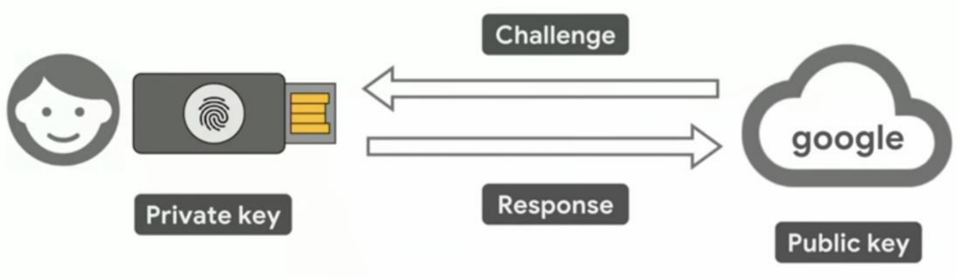
Better Password Policies

Storage

- In a salted and hashed format using a standard library with Argon2id or PBKDF2. see OWASP Cheat Sheet
- Do not invent your own. Obscurity ≠ Security

Just say no to passwords.

- Use a passkey instead. Start with Microsoft or Google.
- Web Authentication API
  - Authenticator device | phone app + fingerprint



Security protects Privacy

- Authentication: MFA (Multi-Factor Authentication)
  - esp. for administration, security, VPN access
- Authorization: Least Privilege Principle
- Enterprise SSO with IdP and MFA via SAML
  - **S**ingle **S**ign **O**n, **Id**entity **P**rovider, **S**ecurity **A**ssertion **M**arkup **L**anguage for authentication and Authorization
- IBM Future of Identity DIACC Ontario-DID

Security protects Privacy

- Systems: Zero Trust Architecture
  - Only Trusted Applications can run on OS
  - Application’s users: “never trust, always verify”
  - Includes server to server inside intranet
- IaC = Infrastructure as Code
- Encrypt **local** *and* backup data
  - So data exported by Ransomware cannot be read for double extortion. Then rebuild from backup.

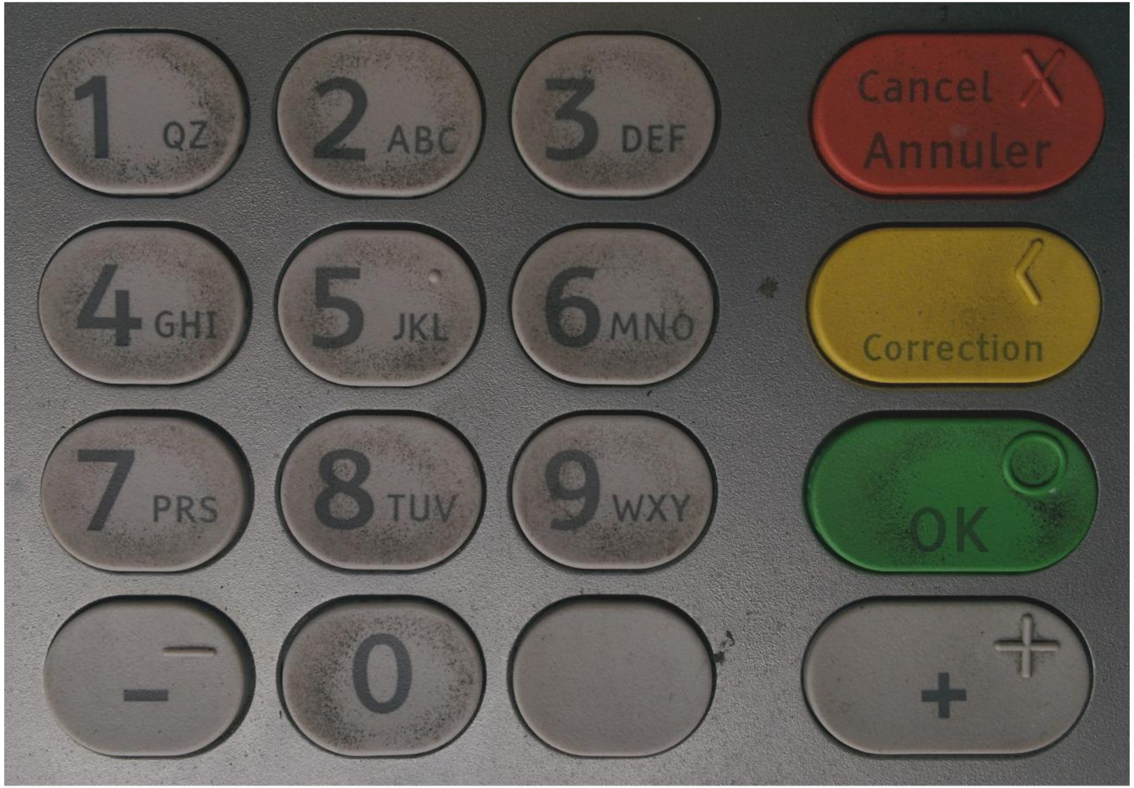
NOTES

…not on the quiz but here for further information and explanation.

PIN: Probably Insecure Number

Input pad at a Toronto ATM. Panel is on a sidewalk open to busy street. Dirt reveals:

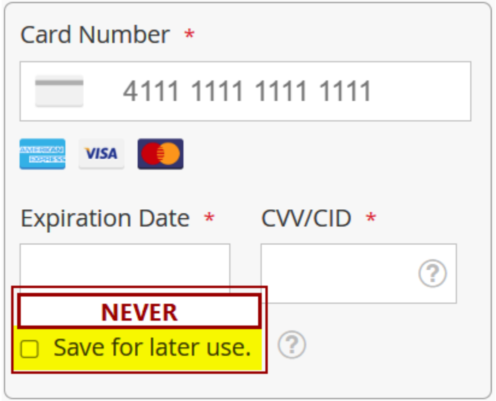
- 1,2,5,7 used most.
- 1,5,7,1 could be a pattern PIN.
- 1,2,3,4 worth a try to crack password.
- 6,8,9 used least.



Safe Payment Practices

Minimize reveal of financial credentials

- Make 'contactless purchases'
  - Use Apple Pay or Google Wallet on smartphone
  - Use Seneca OneCard, prepaid card (Mastercard/Visa), or gift cards
  - Tap payment card to avoid exposing PIN
- eCommerce
  - Use Click to Pay (Mastercard), Visa Secure, PayPal, Amazon
  - Always use 2FA



Card Number *

4111 1111 1111 1111

Expiration Date *

CVV/CID *

NEVER

□ Save for later use.

What happens when free social media meets inadequate security management:

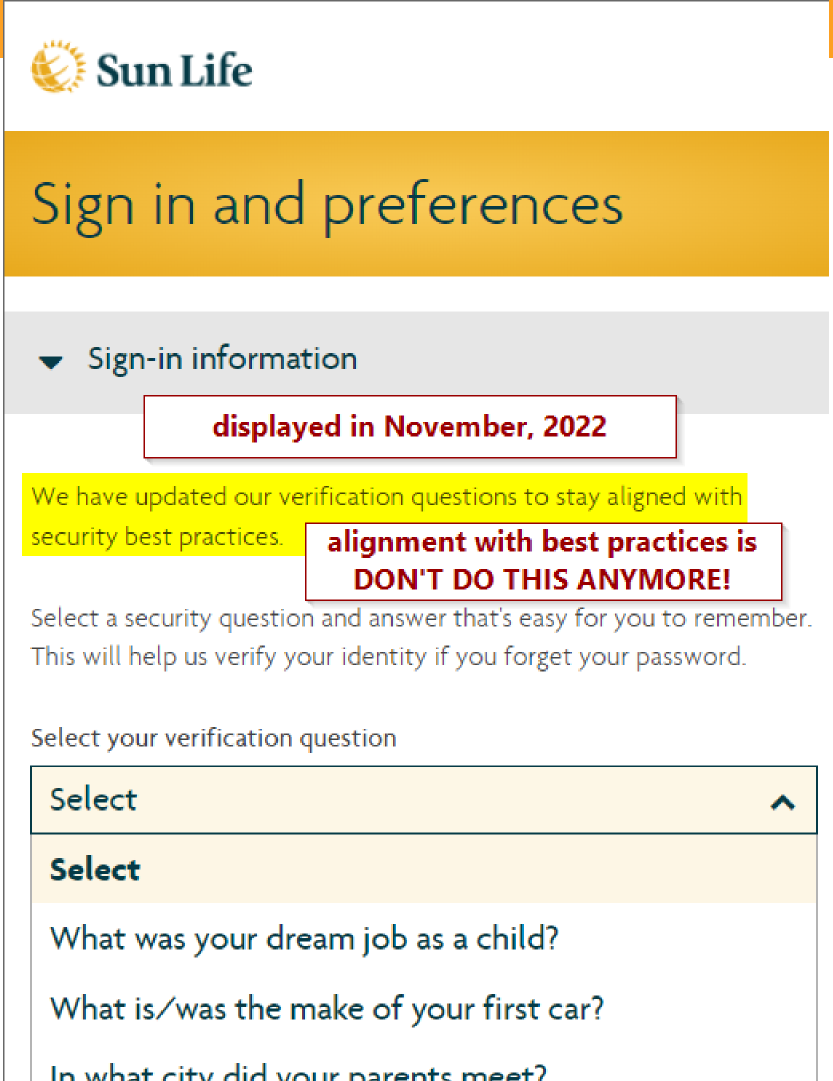
Dear Art Lovers, [*from a professional artist*]

So sad to lose contact with so many of you online.

It has been a crazy few weeks - I have been going down the rabbit hole trying to find a way to get my social media accounts back. From what I have heard, it could take 5 or 6 months...if I am even able to get my accounts back at all. This includes my personal and business Facebook page, my Instagram page, the ArtAlchemyEast Instagram page, as well as the Art Alchemy studio pages.

Between all these accounts, over 9,000 people shared my art journey…

Obsolete practices are still in practice.



Sun Life

Sign in and preferences

Sign-in information

displayed in November, 2022

We have updated our verification questions to stay aligned with security best practices.

alignment with best practices is DON'T DO THIS ANYMORE!

Select a security question and answer that's easy for you to remember. This will help us verify your identity if you forget your password.

Select your verification question

Select

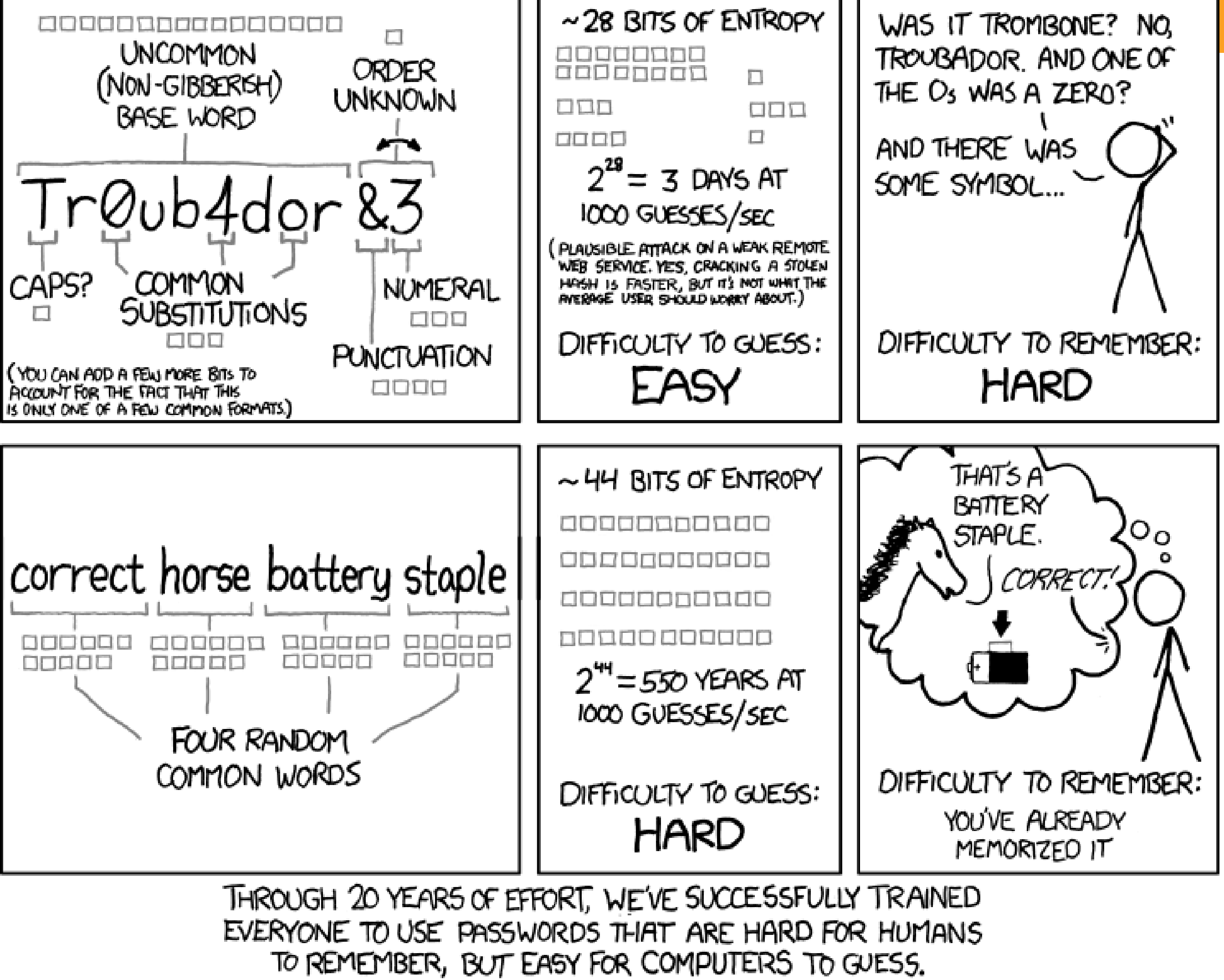
Select

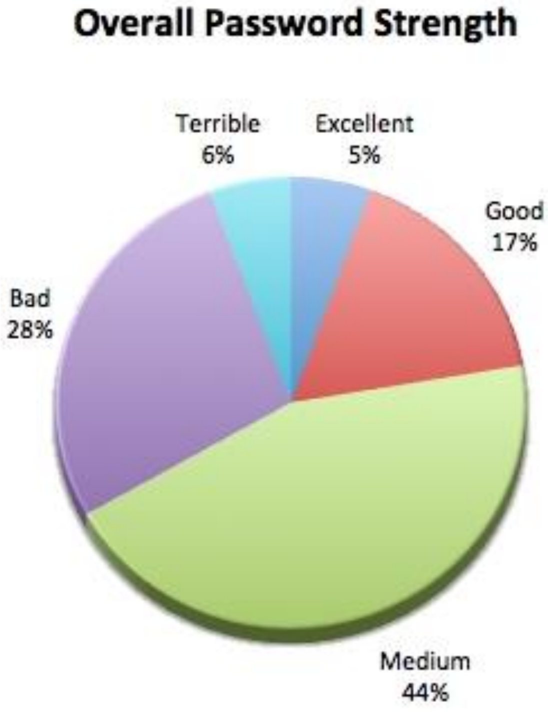
What was your dream job as a child?

What is/was the make of your first car?

In what city did your parents meet?

Sun Life doesn't read the ICT news.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

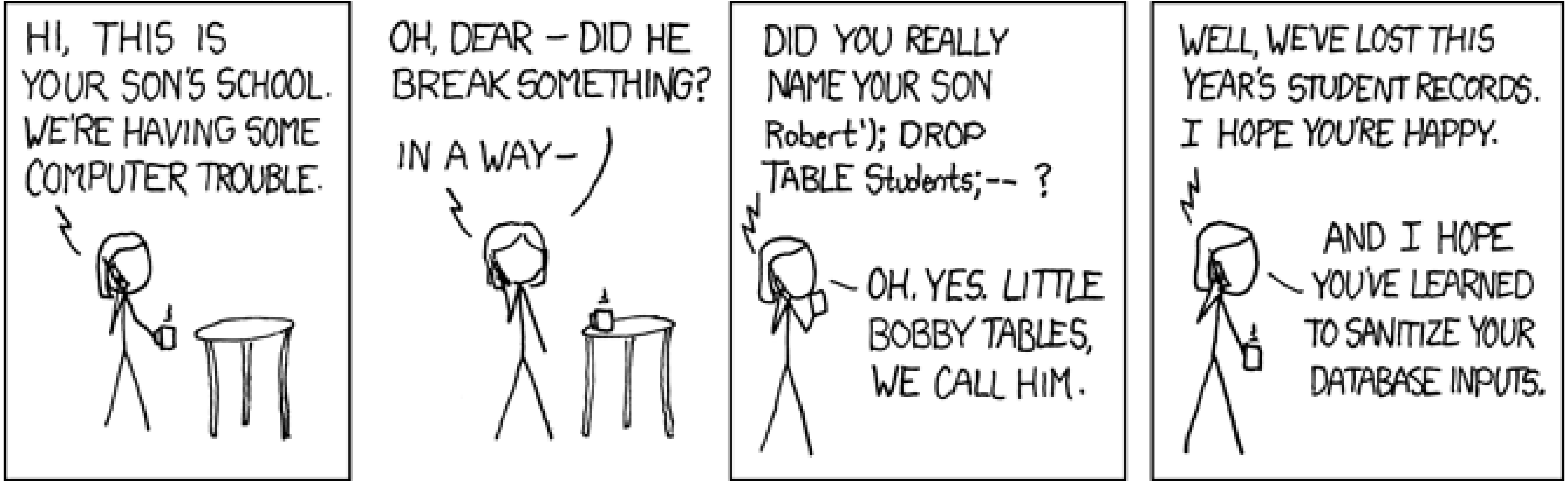


2013 analysis of 2M intercepted logins from real humans.

Security Architecture

- Multi-factor authentication is standard
- Web serving uses micro-services architecture with security baked in.
- Zero Trust model: never trust, always verify.
- segregate client processes from internal resources via highly constricted view of internal network. e.g. only to a switch, or to a port, or to specific services – not to the actual resources themselves such as a DB or file location or to IP addresses of other machines on the network

SQL Injection Attacks


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

- INSERT INTO Students (name) VALUES ('**Robert');DROP TABLE Students;--**');
  - Do not run dynamic SQL statements that include outside data.
- Defence: Use SQL Prepared Statements or parameterized SQL calls. E.g. INSERT INTO Students (name) VALUES ('**?**');

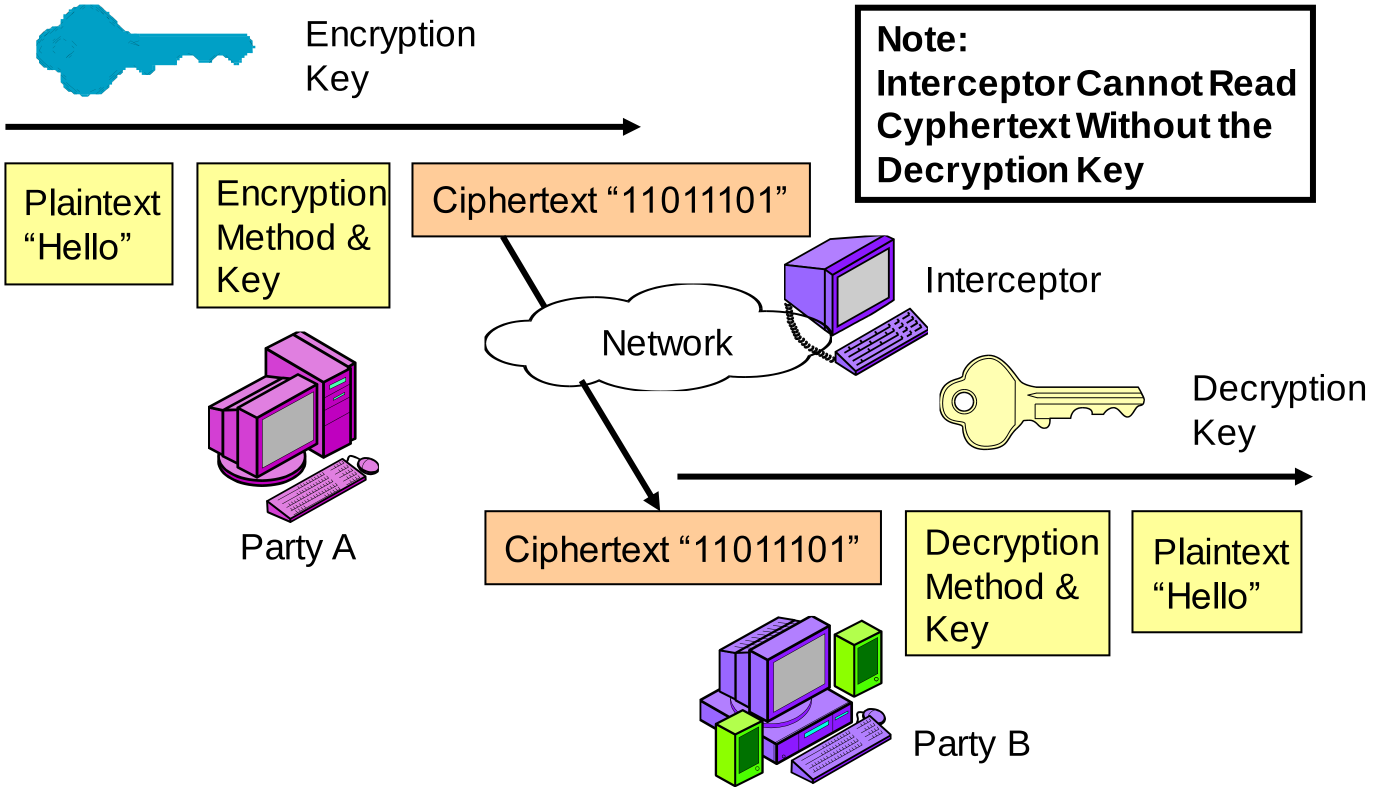
Local and backup security

- Device encryption, e.g. Windows BitLocker or VeraCrypt Works on local drives and/or USB drives.
- The defence against any ransomware is to have backed up your system *yesterday*.
- Backups mean your data has left your system's control and its security and authorization controls. Encrypt all backups.

Safe Online Banking

- Tinfoil Hat: cold boot computer (from powered off state)
- Use only one browser to access financial accounts.
  - Ensure that browser has no add-ins or extensions.
- Open browser with NO TABS, only a plain local page.
- Go into private / incognito mode.
- Do your banking.
- Close the browser.
- Tinfoil Hat: cold boot. In Windows, this now means Restart instead of Shutdown.

Encryption/Decryption Process



Encryption Key

Plaintext “Hello”

Encryption Method & Key

Ciphertext “11011101”

Note: Interceptor Cannot Read Cyphertext Without the Decryption Key

Party A

Network

Interceptor

Decryption Key

Ciphertext “11011101”

Decryption Method & Key

Plaintext “Hello”

Party B

Notes on Authentication

- Authentication is to verify the identity of a user when they log in to a network using a username and password. It is the process or action of “proving or showing something to be true, genuine, or valid.” In Computing World, it is the process or action of “verifying the identity of a user or a process” (mostly used while logging into a computer software/network/website.)

- The network administrator creates an account and assigns a username + password to it.

- The account is usually created when IT receives instruction from HR about a new hire or a change in duties. Mostly a username is based on organization standard and a password is a temporary password which is changed on first login by the user.

Programmer's Perspective of Encryption

- Popular symmetrical encryptions include AES and RC4. Popular Asymmetric encryptions include RSA and ElGamal.

- Many programming languages have libraries for implementing encryption and decryption algorithms to secure data across insecure networks.

- These are just some examples:
  - Jasypt library: a Java simplified encryption library
  - CryptoAPI: .NET encryption library
  - OpenPGP: available for different platforms

What is Encryption?

- Encryption is the “process of converting information or data into a code”, especially to “prevent unauthorized access,” even while data is being transmitted over insecure computer networks.

- In other words, Encryption is a process of encoding or enciphering a message to hide its meaning, called cyphertext, and secure it across insecure networks such as Internet.

- Encryption is the most effective way to achieve data security in transit across insecure networks. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

What is Decryption?

- Decryption is the process of taking encoded or encrypted data and “converting it back” into something (text or other data) that either a human or a computer program can read and understand.

- In other words, Decryption is a process of decoding or deciphering an encrypted message so as to recover plaintext from cyphertext.

What is an “Encryption Algorithm?”

- An **Encryption algorithm** is the sequence of data processing that goes into transforming plaintext into cyphertext (some examples in the next slides.)

- Some Encryption terminology is listed here:
  - **Plaintext**: This is what you want to encrypt.
  - **Cyphertext**: The encrypted output.
  - **Enciphering or Encrypting**: Converting plaintext into cyphertext.
  - **Cryptosystem**: A system for encryption and decryption.

An intro to some types of Encryption Algorithms (Substitutions and Transpositions) with some examples

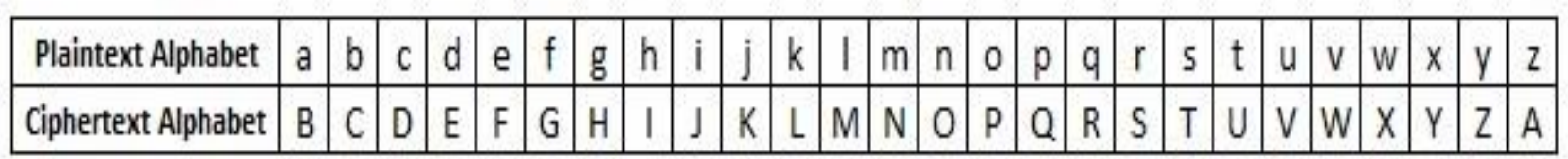
An intro to some types of Encryption Algorithms (Substitutions and Transpositions) with some examples

- All encryption algorithms use a combination of Substitution and Transposition to create cyphertext:
  - Substitutions: One letter of plaintext is replaced with another letter or random symbol. We have Monoalphabetic substitution ciphers (like Caesar ciphers) and Polyalphabetic substitution ciphers (the same plaintext character is encrypted to different cyphertext along the way.)
  - Transpositions or Permutations: The letters are not changed, but the order of the letters is rearranged (e.g. NEXT = ENTX or JOHN = OJNH)

Monoalphabetic Ciphers

- ***Monoalphabetic substitution ciphers*** are based on a fixed replacement structure.

- Using this substitution and the following cyphertext alphabet



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

“Toronto” encrypts to “UPSPOUP”. Note that the frequency of each character is retained which makes simple substitution easy to crack.

Polyalphabetic Ciphers

- ***Polyalphabetic Substitution ciphers*** are based on using multiple alphabets for each character. Let's have an example using the following alphabets:

Plain Alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher Alphabet #1:	B	D	F	H	J	L	N	P	R	T	V	X	Z	A	C	E	G	I	K	M	O	Q	S	U	W	Y
Cipher Alphabet #2:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
Cipher Alphabet #3:	V	Z	A	Y	B	W	C	T	D	S	E	Q	F	J	I	M	N	O	P	G	H	K	L	X	R	U

This time, "Toronto" encrypts to "MLOCMGC" (We use alphabet #1 for the first letter, alphabet #2 for the second letter, alphabet #3 for the third letter, then cycling from the first alphabet again and continue the process to the end of the phrase.)

- ➢ Note that the frequency of the characters is obscured. Even though there are repeated characters they are coming from different alphabets and represent different characters. The more alphabets used, the more random the output.

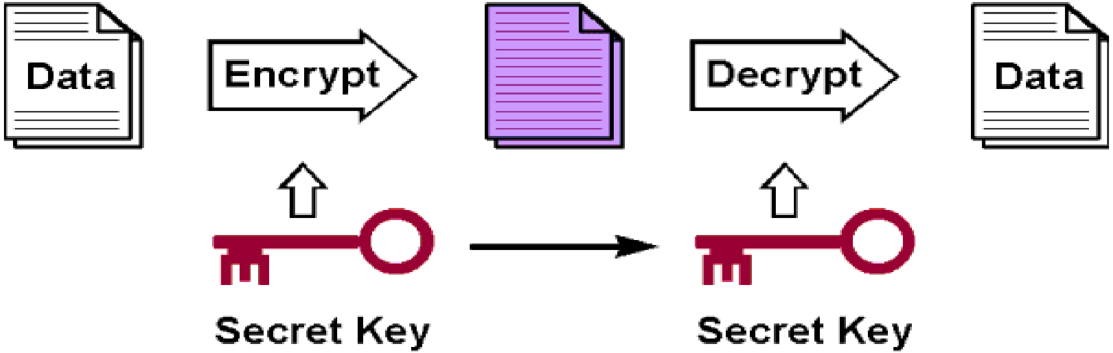
Overview of two types of Cryptosystems (Symmetric/Private Key vs. Asymmetric/Public Key)

Cryptography | NIST
NIST Post-Quantum Cryptography Standardization – Wikipedia
NTRU – Wikipedia

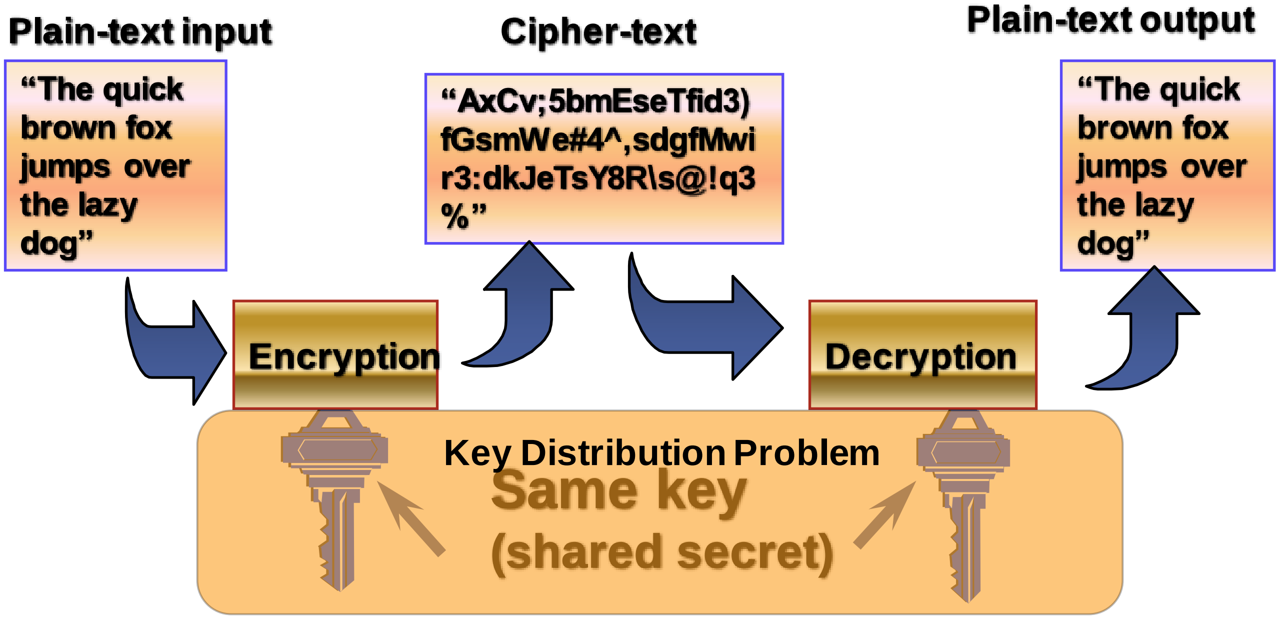
Symmetric Cryptosystem

- **Symmetric Cryptosystem** uses the same key to encrypt and decrypt the message. It is also called “Private Key Cryptosystem”.

- A private or secret key is known only to the parties that exchange secret messages and has to be kept secret for security.



Symmetric Cryptosystem (Cont’d)



Plain-text input

“The quick brown fox jumps over the lazy dog”

Cipher-text

“AxCv;5bmEseTfid3)
fGsmWe#4^,sdgfMwi
r3:dkJeTsY8R\s@!q3
%”

Plain-text output

“The quick brown fox jumps over the lazy dog”

Encryption

Decryption

Key Distribution Problem

Same key

(shared secret)

Symmetric Cryptosystem – Advantages vs. Disadvantages

Advantages	Disadvantages
Very secure if using key greater than 100 bits	Safely distributing key to other party is major concern. Face to Face exchange is best
Keys are shorter than Asymmetric encryption	The number of keys increases exponentially with the number of users exchanging secret information
Very fast performance	If compromised, cracker can decrypt everything -- serious problem

Asymmetric Cryptosystem

- **Asymmetric Cryptosystem** uses two different keys; one to encrypt the message and one to decrypt the message.

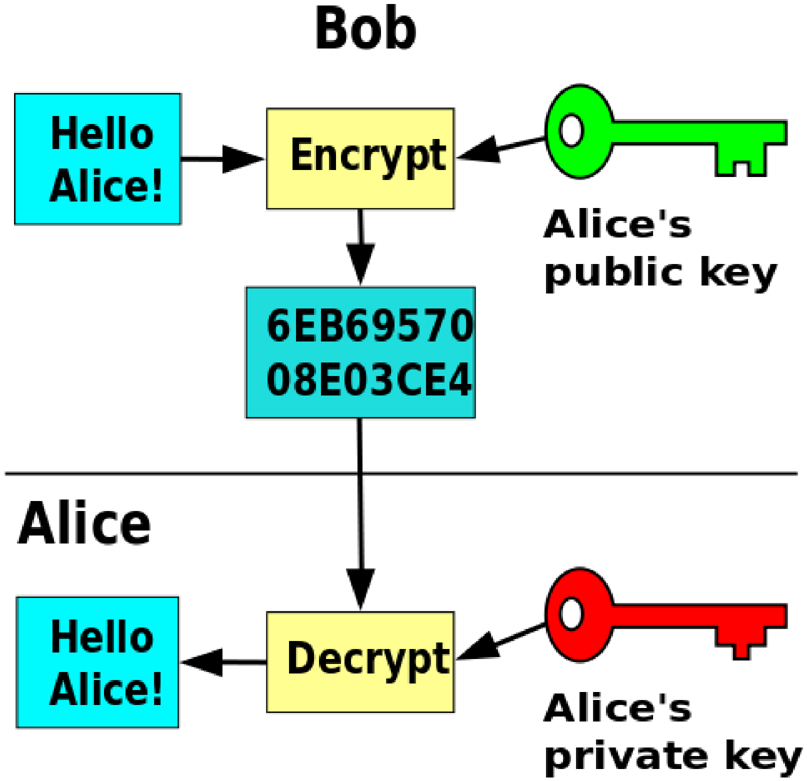
- The keys are mathematically related to each other so that only a message encrypted with the public key can be decrypted with the private key. It is also called “Public Key Cryptosystem”.

- This is a system that uses a public key known to everyone and a private or secret key known only to recipient of the message.

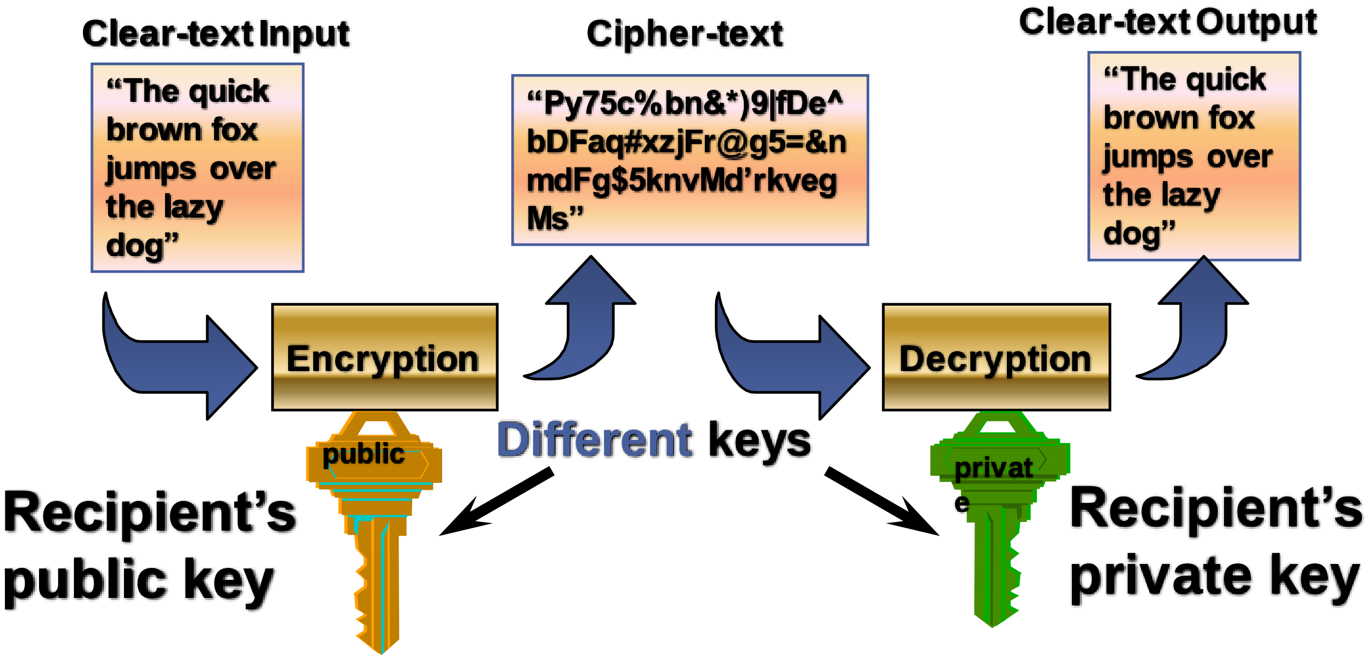
Asymmetric Cryptosystem (Cont'd)

- For Bob to send a secure message to Alice, he uses Alice's public key to encrypt the message.

- Alice uses her private key to decrypt it.



Asymmetric Cryptosystem (Cont’d)



Clear-text Input

“The quick brown fox jumps over the lazy dog”

Cipher-text

“Py75c%bn&*)9|fDe^ bDFaq#xzjFr@g5=&n mdFg$5knvMd’rkveg Ms”

Clear-text Output

“The quick brown fox jumps over the lazy dog”

Encryption

Decryption

Different keys

Recipient’s public key

Recipient’s private key

Asymmetric Cryptosystem – Advantages vs. Disadvantages

Advantages	Disadvantages
Very secure if using key greater than 1000 bits	Each user has one key pair and user's public key is exchanged with all users
Keys are longer because the are exchanged infrequently and public key is shared	If private key compromised, cracker can decrypt messages sent to you, but can not decrypt messages you send to others because encrypted with a different key pair
Slow performance 1000 X slower than symmetric encryption	Requires a key distribution infra-structure

What is Cryptanalysis?

- Cryptanalysis is the study of cryptosystems to find weaknesses in the system which will reveal the plaintext without necessarily knowing the key or the algorithm. This could be done via:
    1. Attempt to recognize patterns in encrypted messages
    2. Attempt to find general weakness in an encryption algorithm

- An encryption algorithm may be breakable, meaning that given enough time and data, a cryptanalyst could determine the algorithm.

➢ If there exists 10^{30} possible decipherments for a given cipher scheme and a computer performs 10^{10} operations per second, finding the decipherment would require 10^{20} seconds (or roughly 10^{12} years)!