Integrity & Basic Encryption

Chapter 6

Krerk Piromsopa, Ph.D. @ 2019

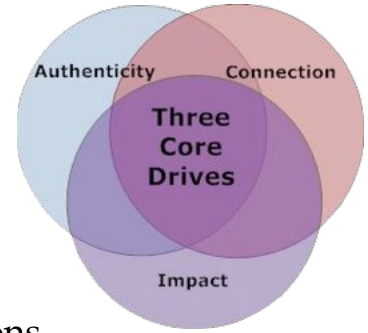
Integrity & Basic Encryption

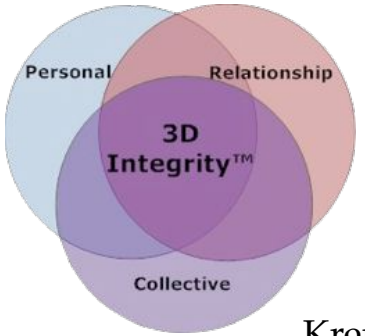
- ★ Definition
  - Integrity, Trust, Sandbox
- ★ Hardware Integrity
  - Physical Tamper Resistance
- ★ Basic Encryption
  - Hash
  - Symmetric Encryption
  - Asymmetric Encryption
  - Public Key
- ★ Security Protocol
- ★ Conclusion

Integrity

"Integrity without knowledge is weak and useless, and knowledge without integrity is dangerous and dreadful."
Samuel Johnson (1709 - 1784)

- ★ Integrity is a characteristic that belongs to people who are self-actualized. It is the quality or condition of being whole, complete, unbroken, and undivided. Knowing oneself heightens a person's integrity.
- ★ Applying to data, it also refers to the state of being whole and undivided or the condition of being unified and unimpaired





Authenticity: the forth A

Integrity requires (hardware) supports.

- ★ Integrity is sometime referred as Authenticity--hence it is sometime mentioned as the forth “A” of security components.
- ★ How can we preserve the integrity of data?

Trust

“Real integrity is doing the right thing, knowing that nobody's going to know whether you did it or not.”
Oprah Winfrey, in Good Housekeeping

- ★ Trust is a basis for every security model.
- ★ I trusted you. What does it mean?
  - believe in the reliability, truth, ability, or strength of [M-W]
- ★ What do you trust?
  - Trust Processor?
  - Trust User/Developer?
  - Trust Software/Process?

Trust-Based System in Action

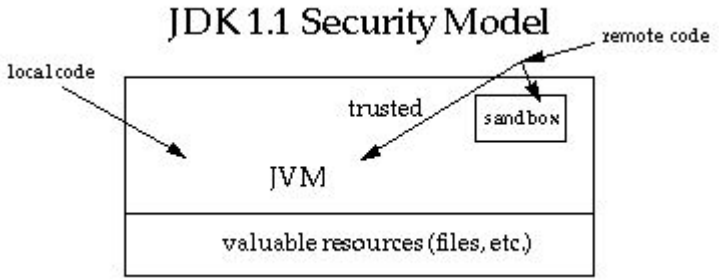
- ★ Single user operating system with no protection (DOS, CP/M, Windows < NT)
- ★ Embedded Systems/Appliances (eg. Air conditioning controller)
- ★ Old mobile phone
- ★ What else?

How to minimize trust?

- ★ In reality, we cannot trust everything.
  So, let's minimize trust.
- ★ Trust with respect to boundary
  - Sandbox
  - Domains (isolation)

Sandbox

- ★ The sandbox security model is popularized by Java (Applet).
- ★ User has an option to trust an applet (remote code). If trusted, the code is run with full local privilege. If not trusted, the code will be in limited a sandbox. (ie. cannot access local files.)



Sandbox (ctd.)

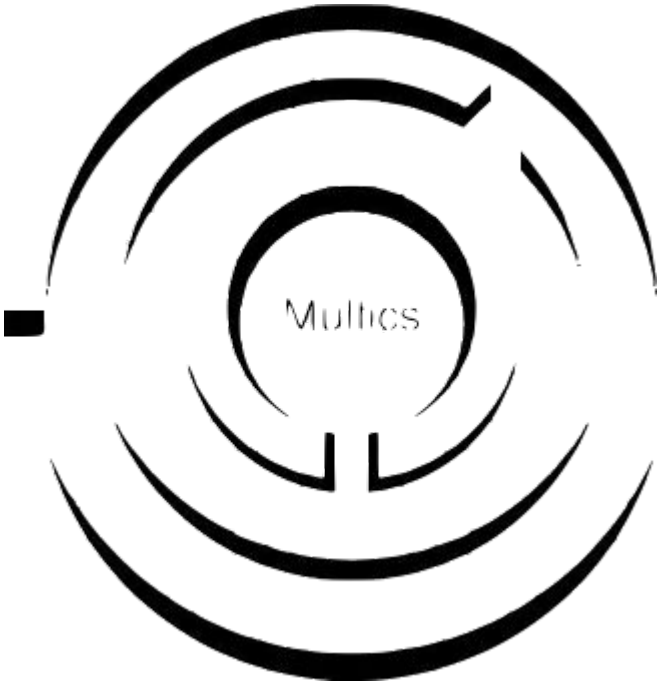
- ★ Trust decision is based on code signing.
- ★ Who do you trust to sign your code?
- ★ Is a signed applet (or ActiveX) a safe program?

- ★ Analogy. Is software that is developed by qualified developer (eg. Microsoft, Oracle) a secure software?
- ★ Trust ≠ Secure

What mechanism is necessary to implement sandbox and/or domain?

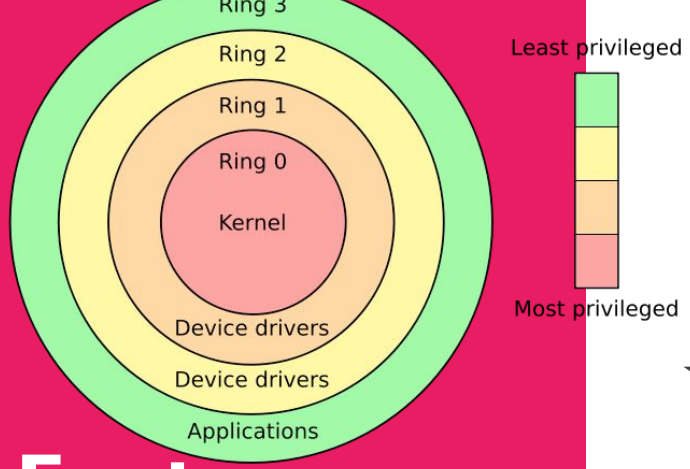
Hardware Support for Integrity

- ★ Electronic curtain
  - Ring
    - Segmentation
    - Page
- ★ Tagged Memory



Ring

- ★ Popularized by Multics (1960)
- ★ Processor provides memory compartments with each part associated with a ring.
  - Segmentation
  - Page
- ★ Inner ring (kernel) can access outer ring. Outer ring cannot only access inner ring though a specific method (ie. system call).
- ★ How many rings do we really need?



Fact

Intel x86 has 4 rings.
Most Operating Systems only use 2 rings (0,3)

★ IBM OS/2 is perhaps the only operating system that deploy device drivers in ring 1 and ring 2.

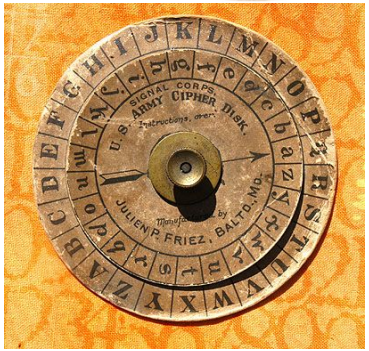
What if there is no hardware support?

Data in a portable drive, email, network packet do not always have hardware protection.

Encryption as a tool

History of Encryption

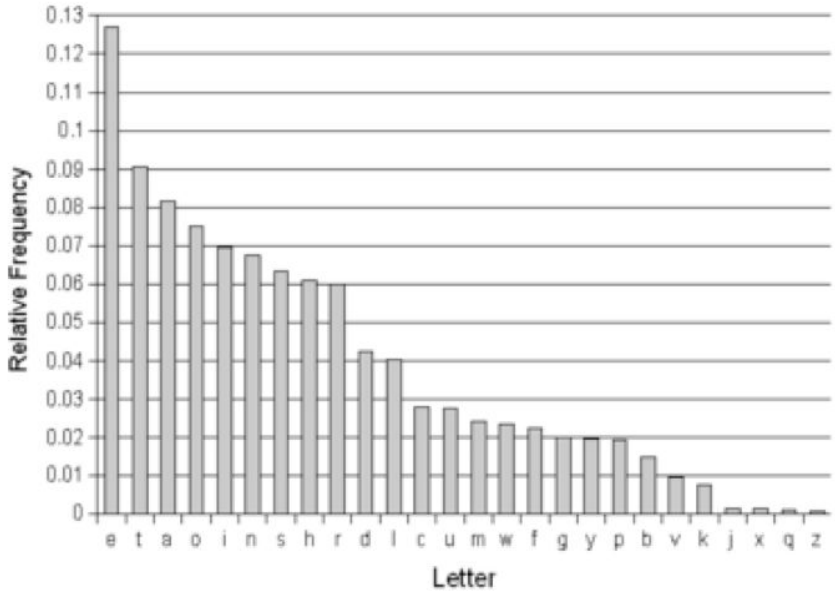
- Monoalphabetic Substitution Cipher
- Julius Caesar (50 BC) used it.
  - Abcdefghijklmnopqrstuvwxyz
  - SECURITYABDFGHJKLMNOPQVWXZ
- What is...? YRFFJ VJMFU



Pictures taken from
https://www.amazon.com/DIY-Escape-Room-Bundle-Experience/dp/B08DJGM87T?ref_=ast_sto_dp
https://people.duke.edu/~ng46/collections/crypto-disk-strip-ciphers.htm

Weakness of Encryption

★ Given a sufficiently large encoded message, it can readily be "cracked" by comparing the frequency of letter occurrences in the coded message with the frequency of letter occurrences in the language used for the message.



Try this

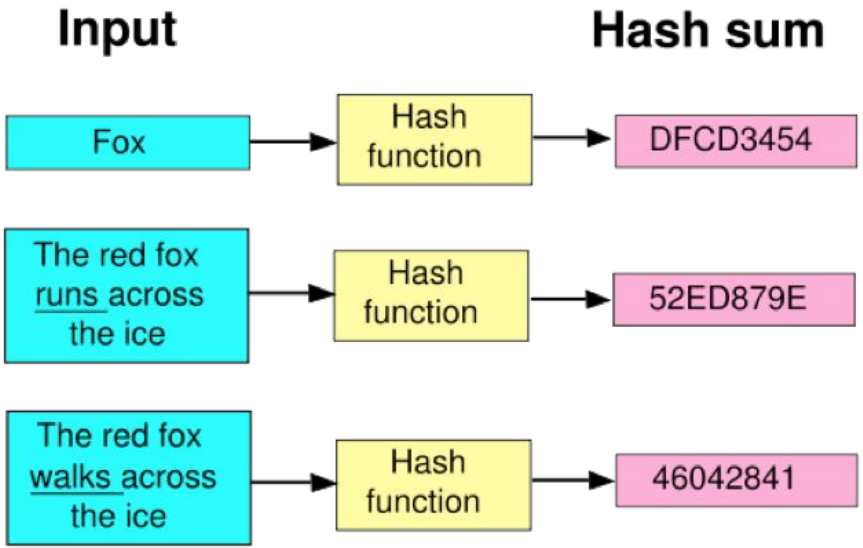
```
Gur fbyhgvba gb gur pvcure vf gur anzr nhoerl juvpu jnf
qvssvphyg gb fbyir orpnhfr yvfgf bs cgbyrzl pbafgryyngvbaf
jrer vapbafvfgrag. Vg gbbx frireny snvyrq nggrzcgf orsber
svaqvat n jbexnoyr yvfg.
```

Encryption in Modern Day

- ★ Hash Digests (short input > long output)
  - Message Digest (MD5, SHA-1, SHA-256, SHA-512, Tiger-Hash)
- ★ Symmetric Encryption
  - Stream Cipher
    - eg. RC4 (used in SSL, WEP, WPA, etc...)
  - Block Cipher
    - eg. AES, Blowfish, DES
- ★ Asymmetric Encryption
  - Public Key
    - RSA
    - DSA

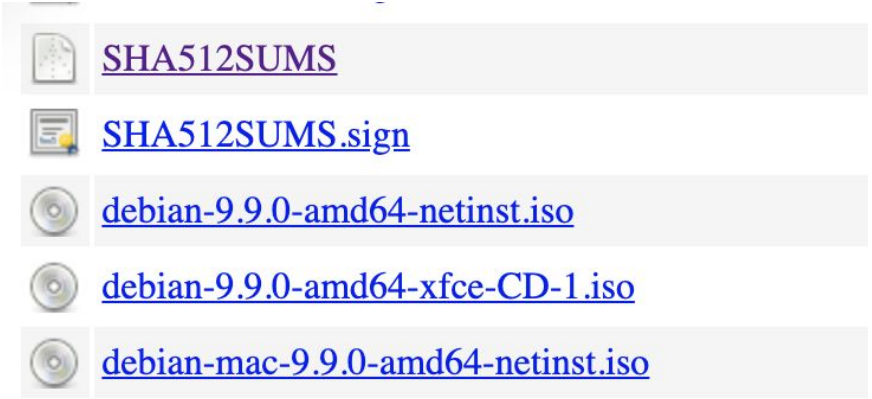
Hash (aka. Message Digest)

- ★ Hash is a one-way function. (Theoretically no inverse function)
- ★ Input may vary in size, output is a fix-length value.
- ★ Collision?



Food for Thought: Hash and Integrity

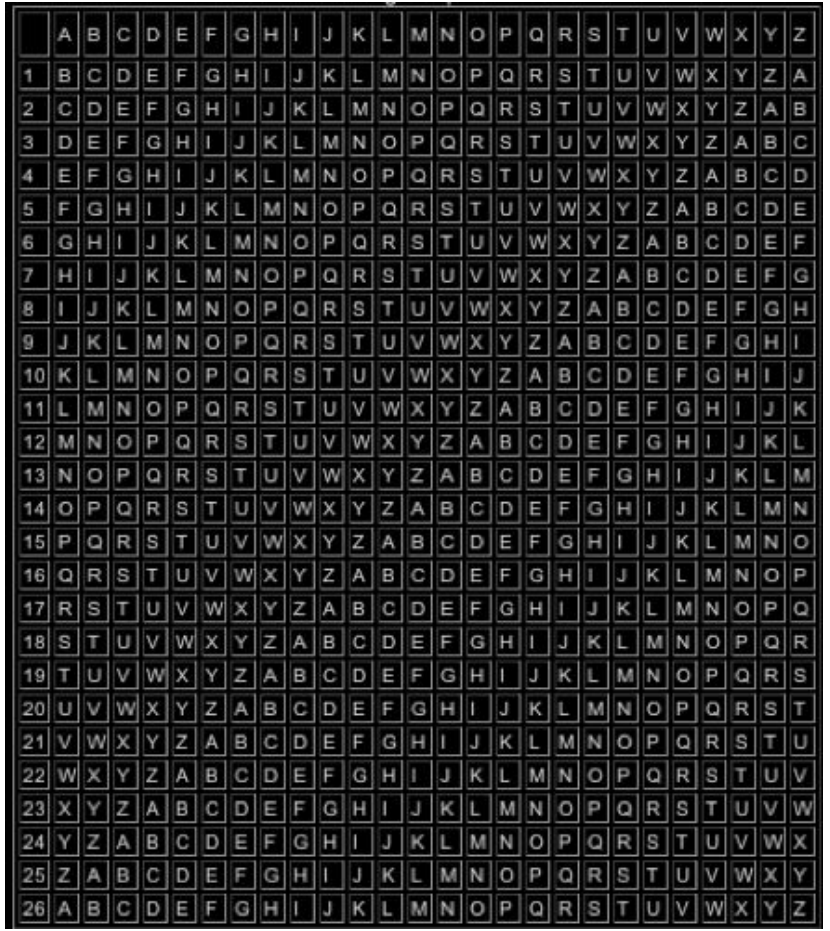
- ★ Hash Value is used widely for integrity check.
  (Eg. To validate that software downloaded from mirror sites is the same as the original software.)
- ★ Since it cannot be decrypted, hash is sometime not considered an encryption.



Stream Cipher

- ★ Vigenere (1467) is among the first stream cipher.
- ★ Extend the key to match the size of input.
- ★ Depending on a position, a same letter may encrypt differently.

LUCKYLUCK ---- Key (extended)
COMPUTING ---- Plain Text
NIOZSECPQ ---- Cipher Text



Block Cipher

- ★ Wheatstone-Playfair Cipher (1854)
- ★ Use heavily during the World War II
- ★ Construction 5x5 cipher blocks.
- ★ Grouping data in two, and use the corner to encode data.
- ★ Depending on a group, a same letter may encrypt differently.

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Example,

CO MP UT ER

OW EO ZD GE

For more details, see https://en.wikipedia.org/wiki/Playfair_ciphe

Mode of Operation in Block Cipher

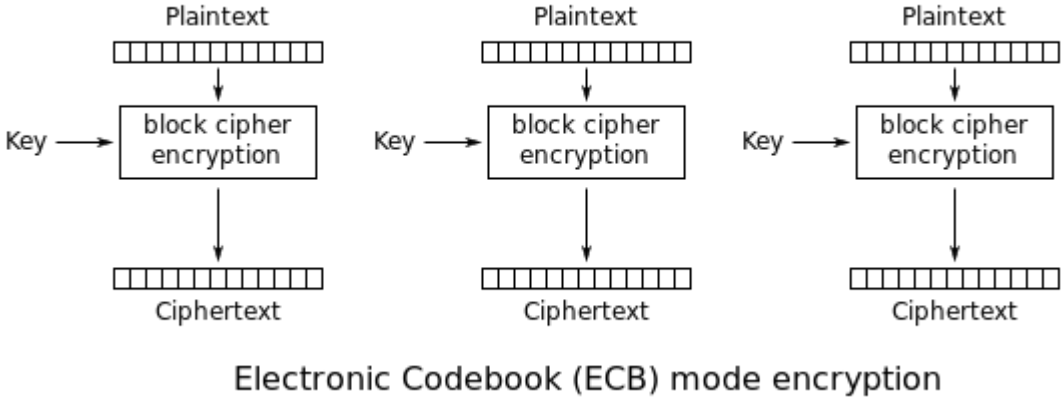
- Variations
  - Initial Vector
  - Padding
  - Chaining
  - Feedback
- Some modes may still be easier to find patterns.

- **Electronic codebook (ECB)**
- **Cipher block chaining (CBC)**
- Propagating CBC (PCBC)
- **Cipher feedback (CFB)**
- **Output feedback (OFB)**
- Counter(CTR)
- Galois/Counter (GCM)

Electronic codebook (ECB)

Block to Block without feedback or IV

Pattern is still there?



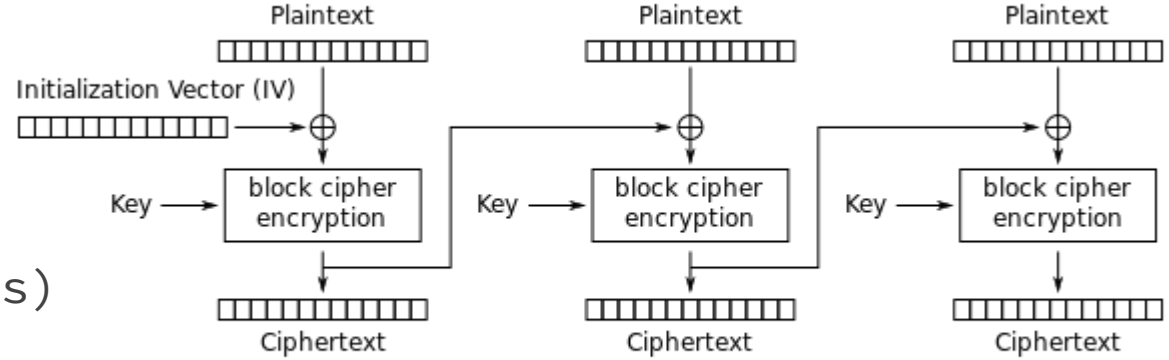
Electronic Codebook (ECB) mode encryption

Original

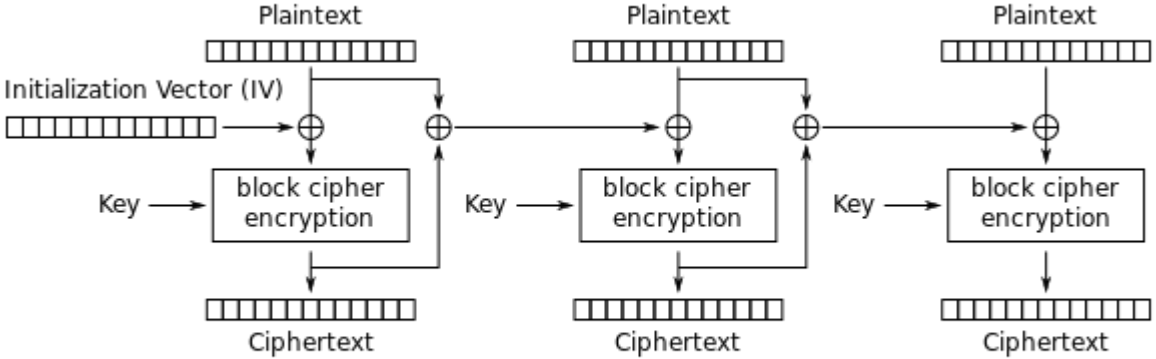
aes-256-ecb

CBC & PCBC

★ CBC (and variations) includes IV.



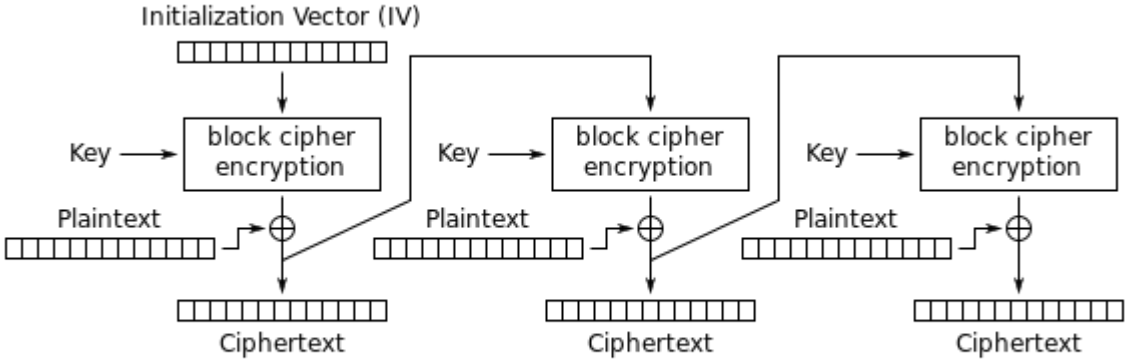
Cipher Block Chaining (CBC) mode encryption



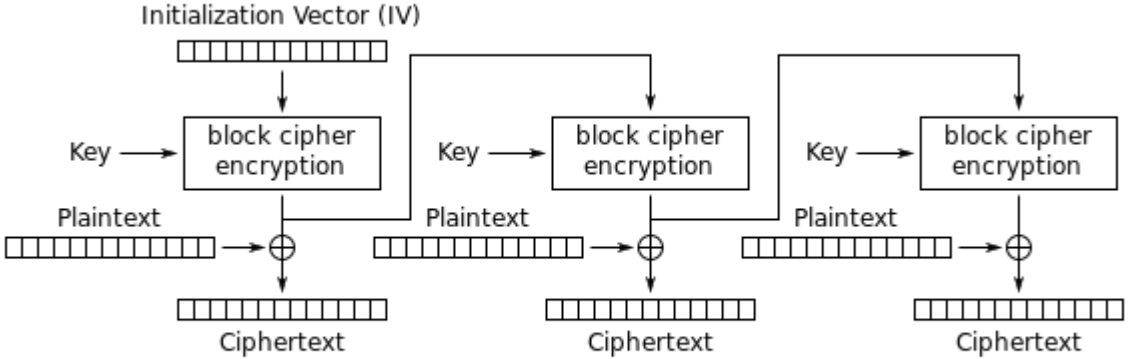
Propagating Cipher Block Chaining (PCBC) mode encryption

CFB & OFB

★ CFC (and variations) includes IV and use output as a feed for next block.



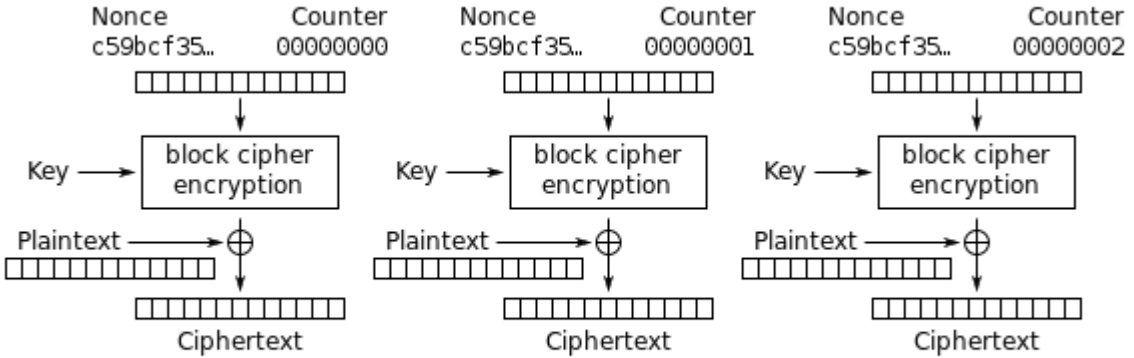
Cipher Feedback (CFB) mode encryption



Output Feedback (OFB) mode encryption

Counter

★ Counter (and variations) use counter and nounce as a vector for each block.



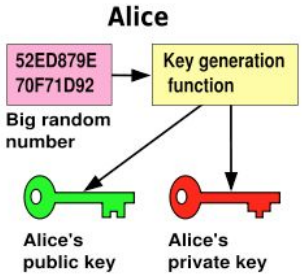
Counter (CTR) mode encryption

Food for Thought: Scalability of Symmetric Encryption

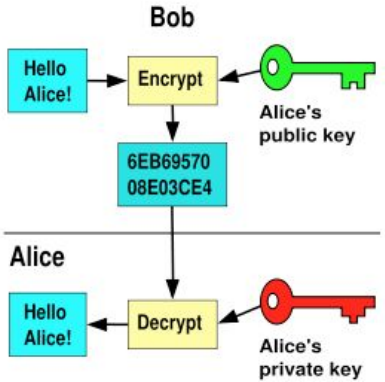
- Assuming that a professor wants to share a piece of information with 100 students, how many (symmetric) key do we need in order to prove the integrity of the information? (ie. proof that the document is created by a professor and only the professor.)

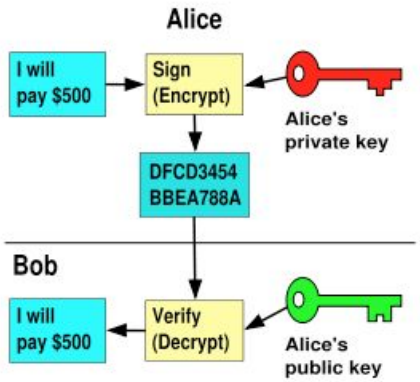
- Hint.
  With one key, anyone (with the key) can write a message.

Public Key



- ★ Based on prime numbers, a key pair (private key and public key) is created.
- ★ Message encrypted with a private key can only be decrypted with the associated public key--vise versa.





Public Key (ctd.)

- Now, we only have to keep the private key. Our public key can freely be distributed. (eg. posted on our personal page.)

- Note that there is still an issue with the physical identity of the public key owner.

Food for Thought: Public Key

- Bob wants to send a message to Alice in a way that only Alice can read and Alice can proof that the message is coming from Bob. How?

  (Which one is more secure?)

  - A. $((\text{message})_{\text{Bob's Priv}})_{\text{Alice's Pub}}$
  - B. $((\text{message})_{\text{Alice's Pub}})_{\text{Bob's Priv}}$

Fact

Public Key is slow.
Block/Stream Cipher is faster.
Hash function is the fastest.

★ Algorithmically, Public Key is based on exponential functions. It is slow. Stream Cipher and Block Cipher are based on logic function. It is faster.

Fact

Encryption for Authentication and Authorization.

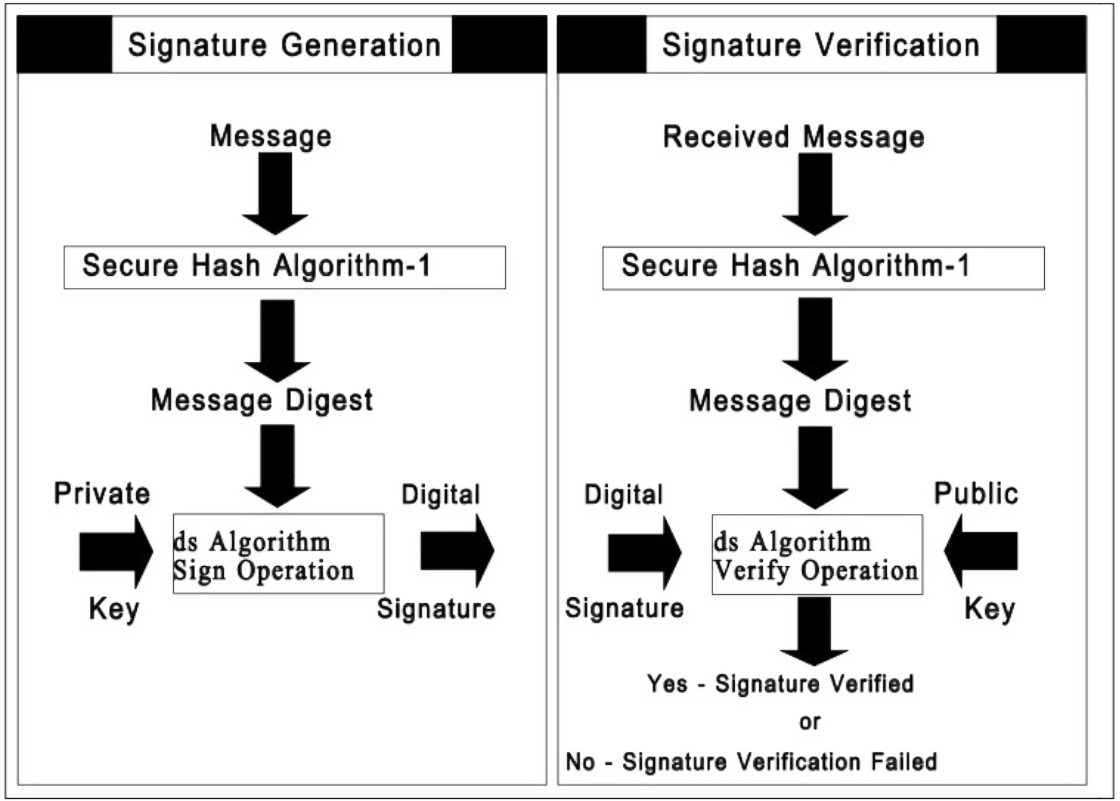
- With proper key management, encryption can provide both authentication and authorization.
- For authorization, it can provide both confidentiality and integrity.
- However, encryptions are vulnerable (to statistical analysis). With enough processing power, everything can be cracked.

Security Protocol

★ Security Protocol is usually a combination of several encryption algorithms. They usually combine pros and cons of several algorithms.

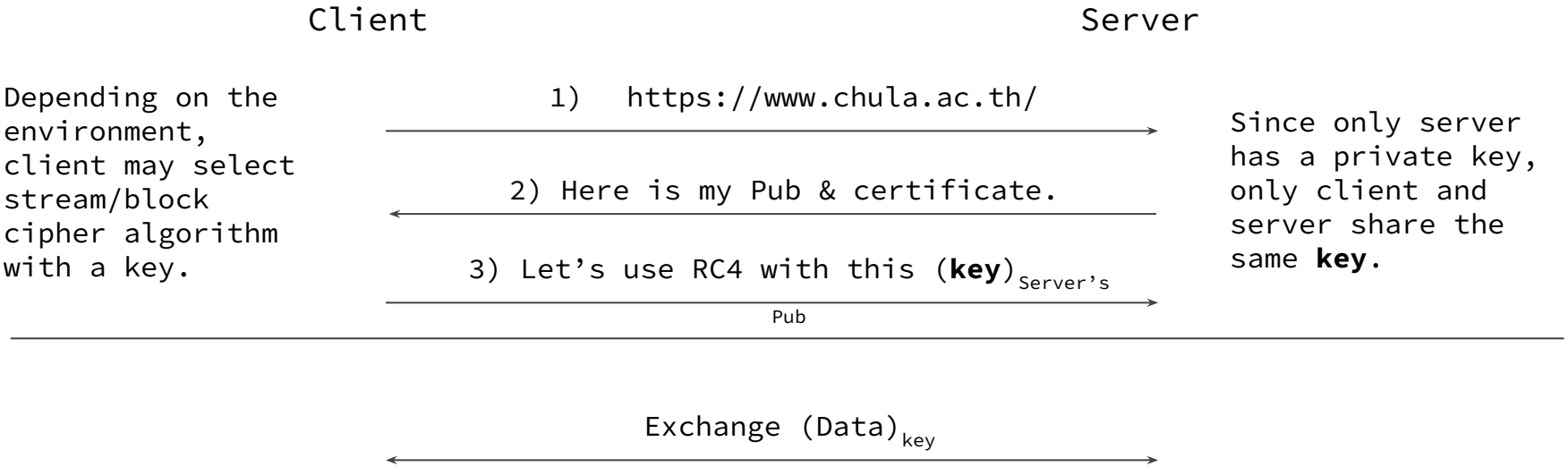
Security Protocol: Digital Signature

- ★ A receiver can verify the originality of the a (plain) text.
- ★ Combine the speed of message digest with the scalability of public key.



Security Protocol: HTTPS/SSL/TLS

★ Combine speed of symmetric key with scalability of public key.



SSL/TLS Protocol

Note: We will revisit the certificate later.

Pop Quiz

★ What kind of security do we get from encryption?

★ Most people think that encryption is secure.
Do you agree or disagree?

Conclusion

- ★ Integrity requires either hardware support or encryption.
- ★ A combination of hardware and Operating System serves as a basis for integrity (security).
- ★ A box with strong integrity means it will always keep things inside in the original conditional for years.
- ★ There is not absolute integrity. Most of the time, a security breach is the break of integrity. (eg. A thief broke a window and got into a property.)

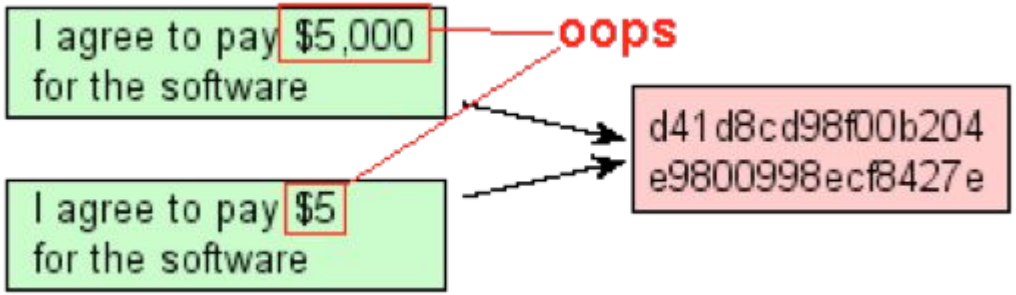
Conclusion (ctd.)

- ★ Contemporary Algorithms
  - Hash/Digest Algorithms
    - ~~MD5, SHA-1~~, SHA-256, SHA-512
  - Stream Ciphers
    - RC4, CHACHA, SEAL
  - Block Ciphers
    - Blowfish, DES, 3DES, AES
  - Public Key
    - RSA, DSA

Conclusion (ctd.)

★ Other issues not in this chapter:

- Key management (We will revisit this in PKI later.)
- Collision of hashing function
  http://www.mathstat.dal.ca/~selinger/md5collision/
- Post-Quantum Encryption
- Elliptic-curve cryptography



End of Chapter 6