Cyber Physical System Security SC4015/CE/CZ4055

Anupam Chattopadhyay

CCDS, NTU

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

Discussions from Last Week

1. Go to wooclap.com
2. Enter the event code in the top banner

Event code
CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Automata and *Examples*

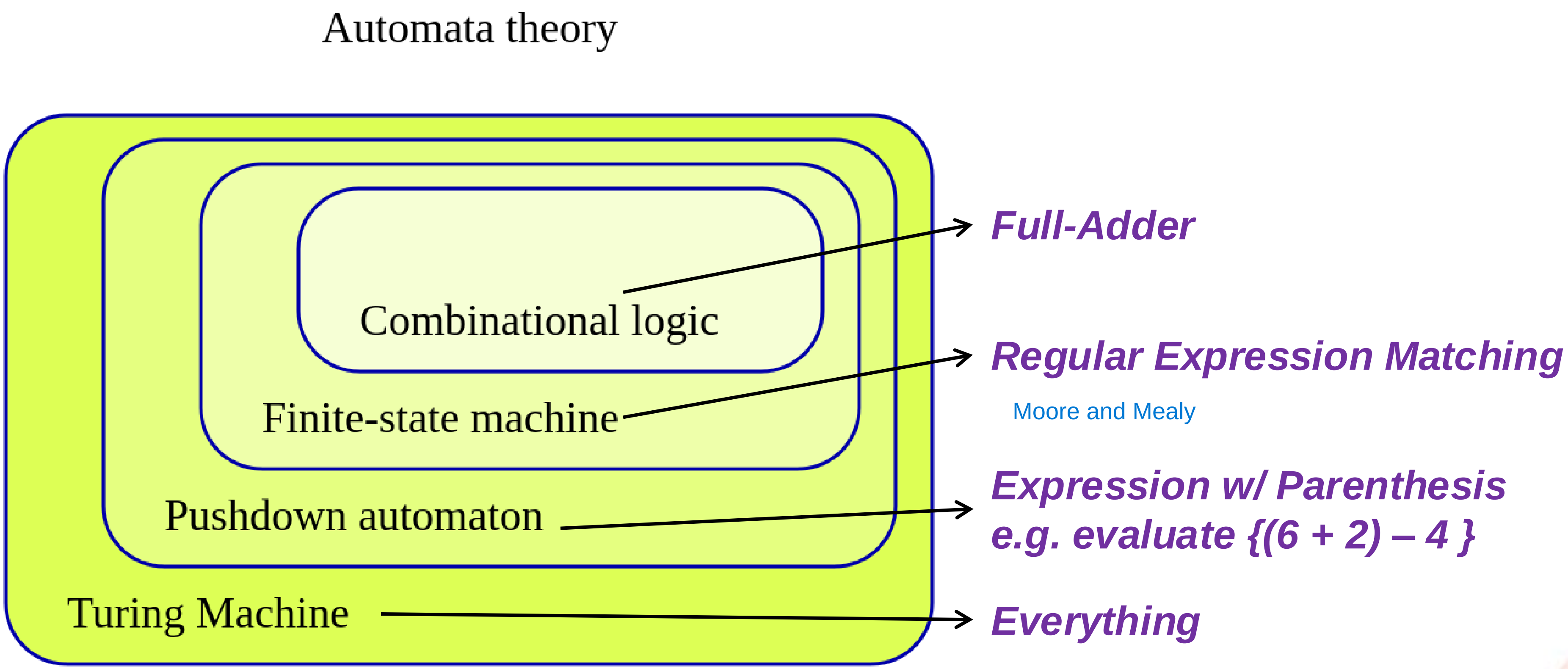


Image source: wikipedia

NANYANG TECHNOLOGICAL UNIVERSITY

Trusted Service Manager

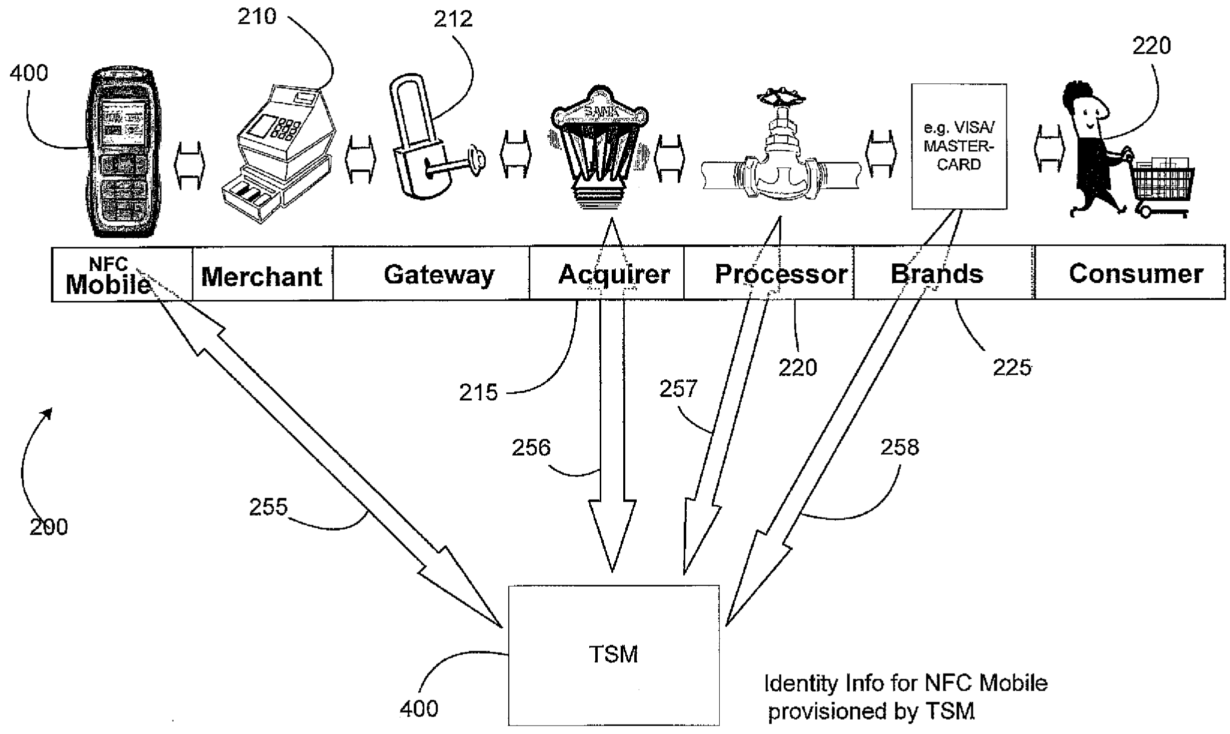


FIG. 2

Image source: Paypal patent US8417643B2

Trusted Service Manager

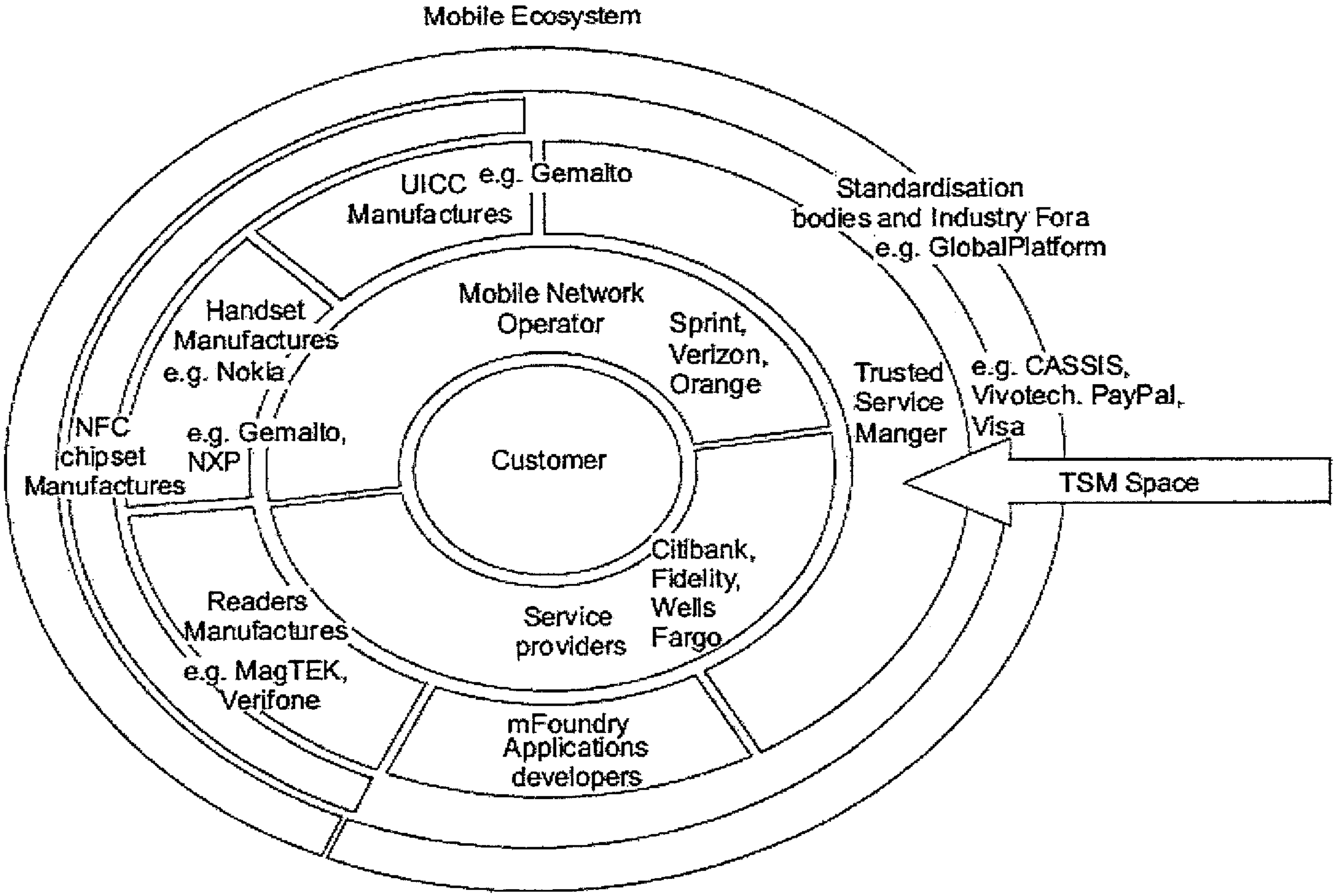


FIG. 1

Image source: Paypal patent US8417643B2

Trusted Service Manager: Tasks

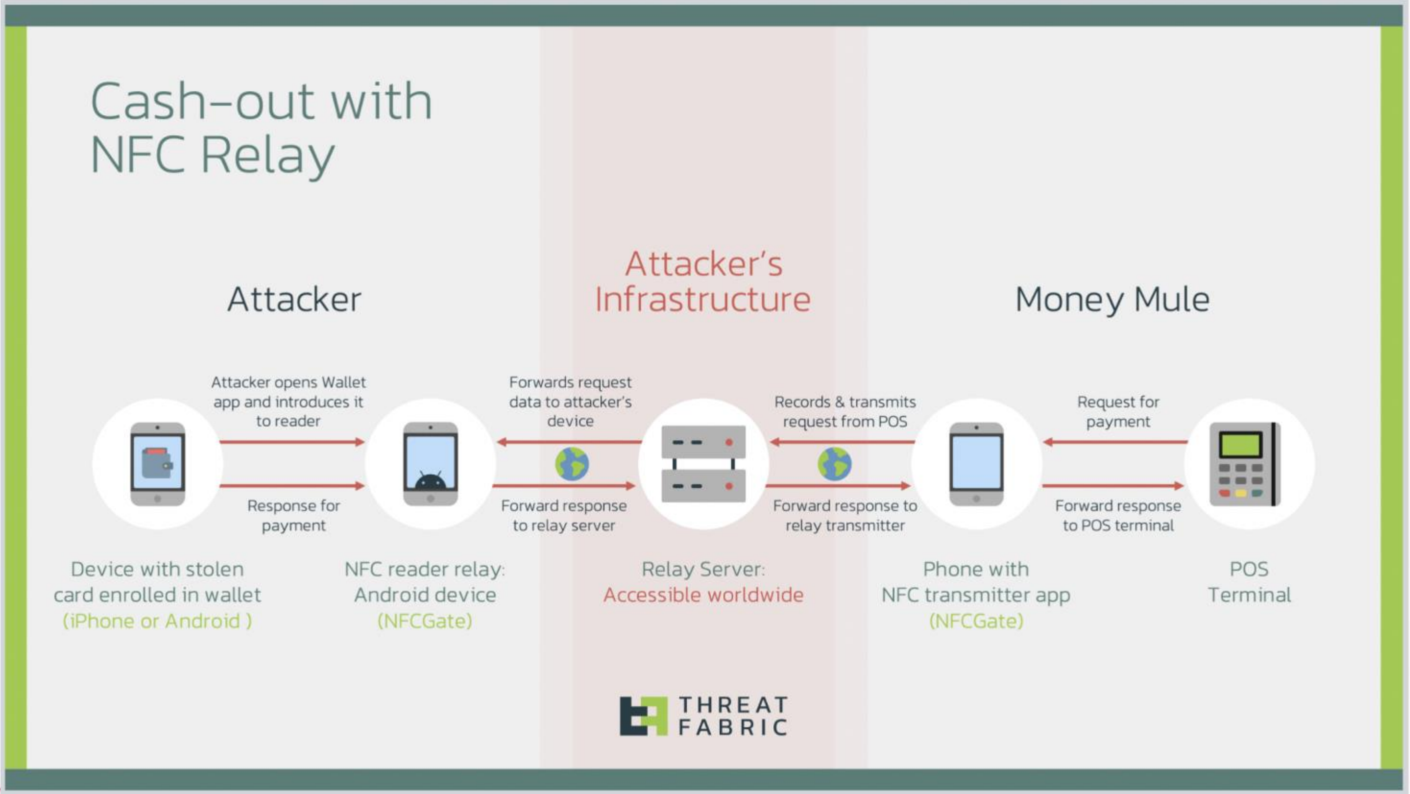
1. **User registration**: Corresponding to a bank
2. **Managing Digital Certificates**: User identity
3. **Authentication** and **Verification**: Transactions of the mobile wallet with a payment terminal

- The above services are delivered using the underlying platform, in particular
  - **SE**: Storage of keys, passwords, identity
  - **Secure Communication**: NFC
  - **TEE**: Secure Microprocessor for providing security services (e.g., encryption, authentication)

NANYANG TECHNOLOGICAL UNIVERSITY

NFC Security *(1/2)*

- NFCGate: Android toolkit for NFC traffic (and security) analysis
- Used by hackers to steal money

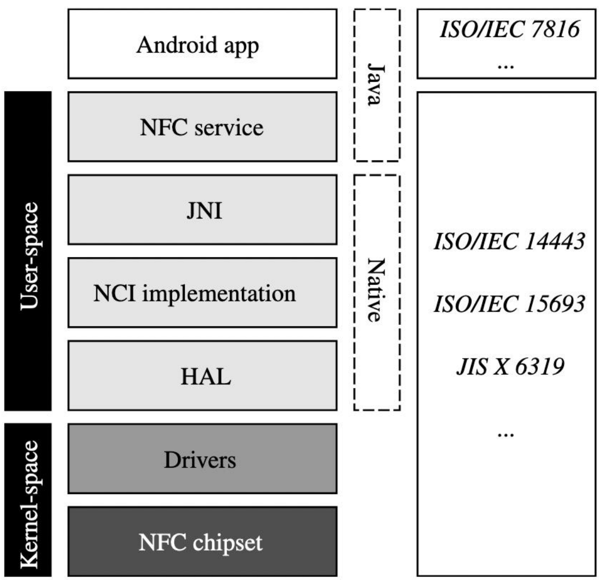


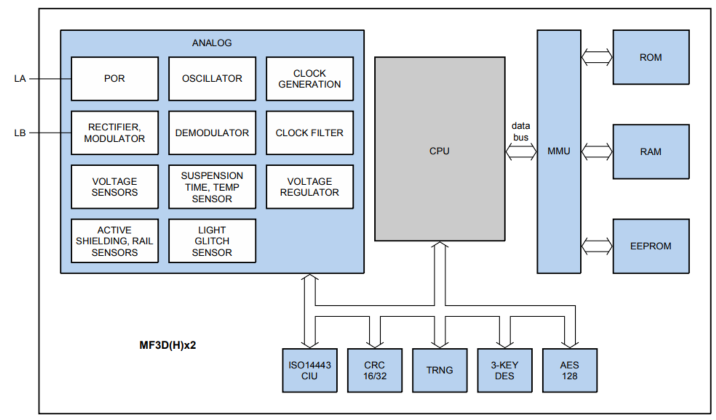
NANYANG TECHNOLOGICAL UNIVERSITY

S. Klee et al, "NFCGate: Opening the Door for NFC Security Research with a Smartphone-Based Toolkit", Usenix 2020
https://thehackernews.com/2024/11/ghost-tap-hackers-exploiting-nfcgate-to.html
https://github.com/nfcgate/nfcgate/blob/v2/doc/Compatibility.md

NFC Security *(2/2)*

- Through *Java symbolic hooks* → from other applications running in the background of the same platform
- Through *native instruction hooks* → alter the underlying platform behavior





Reverse engineer packets, as NFC IC is known

S. Klee et al, "NFCGate: Opening the Door for NFC Security Research with a Smartphone-Based Toolkit", Usenix 2020
https://thehackernews.com/2024/11/ghost-tap-hackers-exploiting-nfcgate-to.html
https://github.com/nfcgate/nfcgate/blob/v2/doc/Compatibility.md
https://github.com/nfc-tools/libfreefare

NANYANG TECHNOLOGICAL UNIVERSITY

NFC Security: Countermeasures

- Preventing Relay Attack

- Do not let *untrusted apps* running in the background
- Distance Bounding Protocols
  – To ensure that the endpoints of a communication are within a specified distance
- Mandatory Response Timeouts
  – To ensure that the reader ends a communication when there is a significant time-lag (introduced due to the relay)

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- *Security Triad*
- Cryptographic Primitives
- Discussion

1 Go to wooclap.com

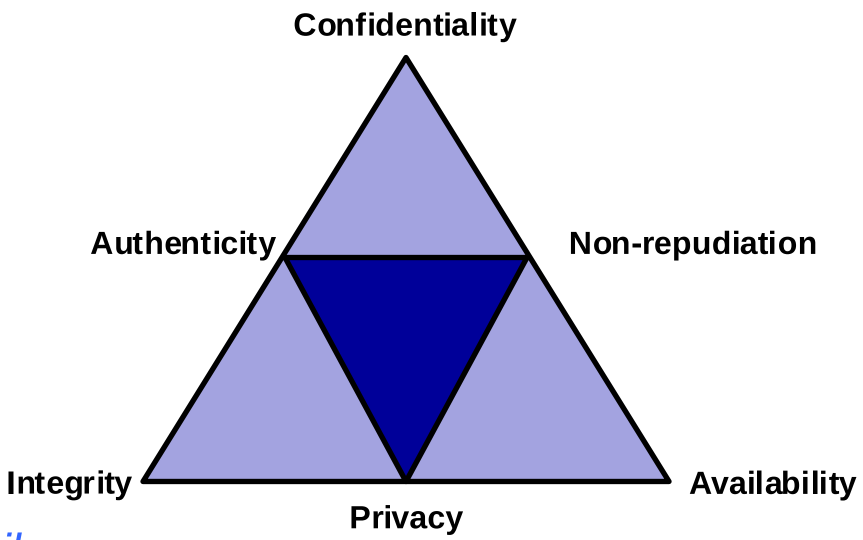
2 Enter the event code in the top banner

Event code
CPSSECURITY

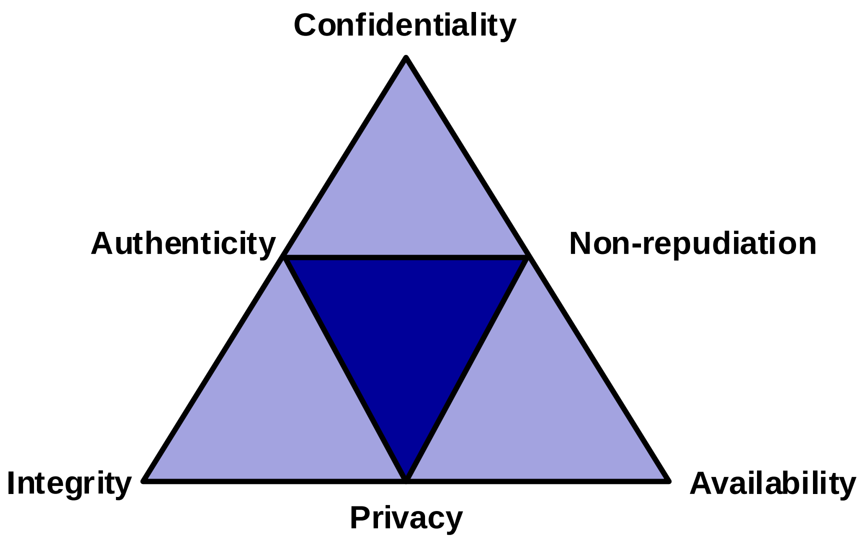
NANYANG TECHNOLOGICAL UNIVERSITY

Security Triad

- IT security
  - Confidentiality
    - *Data is secured*
  - Integrity
    - *Data is trusted*
  - Availability
    - *Data is accessible*
  - Non-repudiation
    - *Service has a trusted audit-trail*
  - Authenticity
    - *Components have provable identity*
  - Privacy
    - *Service does not see customer activities*



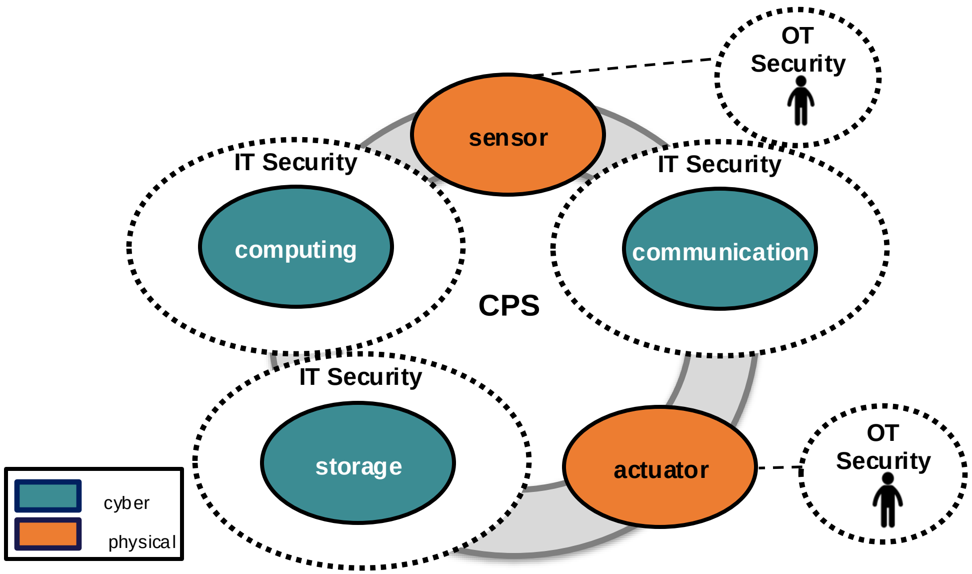
Security Triad: Smart Card

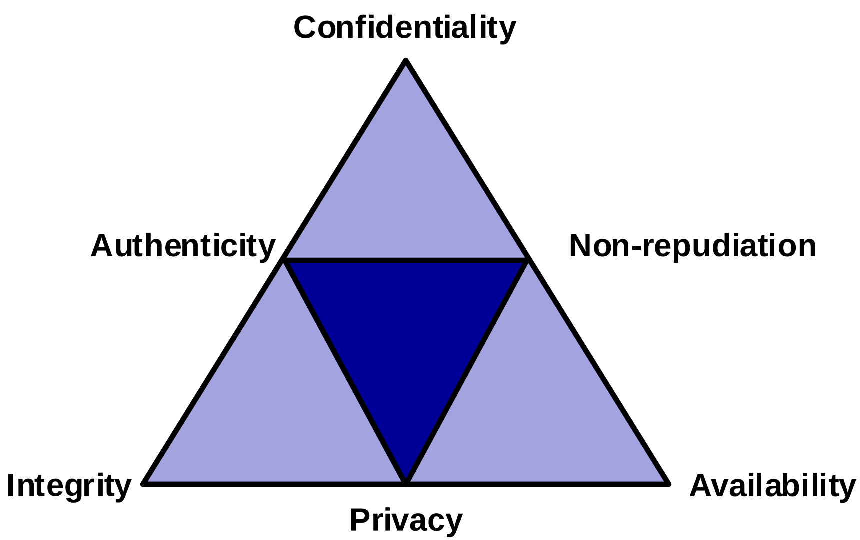


- Smart Card security
  - Confidentiality: *Data is secured*
  - Integrity: *Data is trusted*
  - Availability: *Data is accessible*
  - Non-repudiation: *Service has a trusted audit-trail*
  - Authenticity: *Components have provable identity*
  - Privacy: *Service does not see customer data*

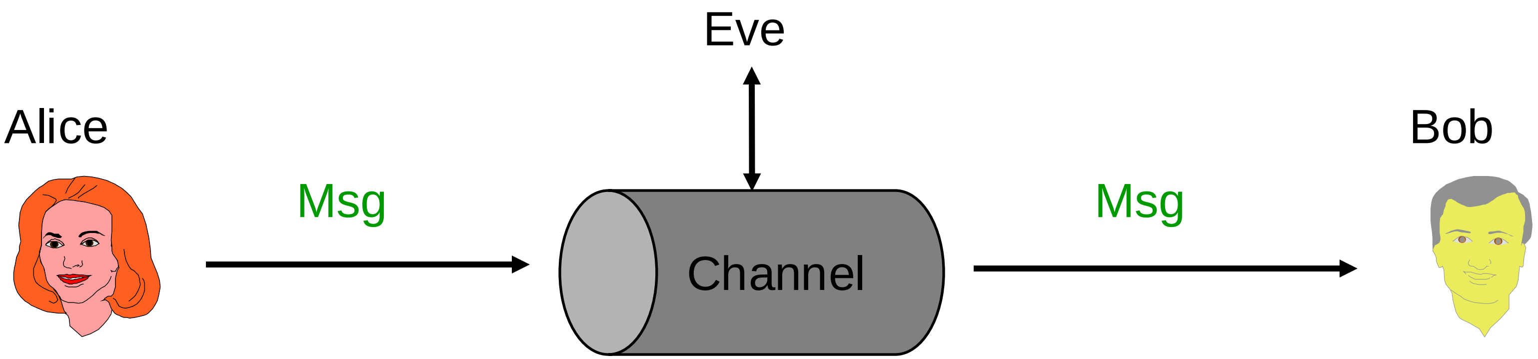
NANYANG TECHNOLOGICAL UNIVERSITY

Security Triad for CPS



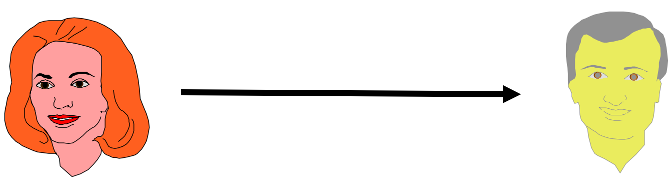


Network Security Model

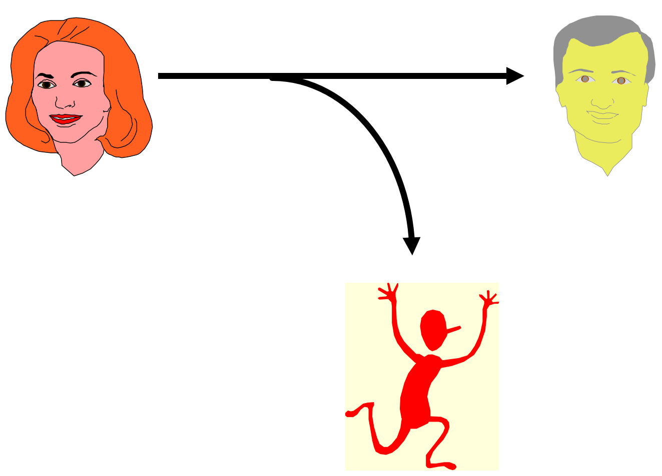


Confidentiality (Secrecy)

- Protect transmitted data
- Protect against traffic analysis



- **INTERCEPTION**
  Unauthorised party gains access to data

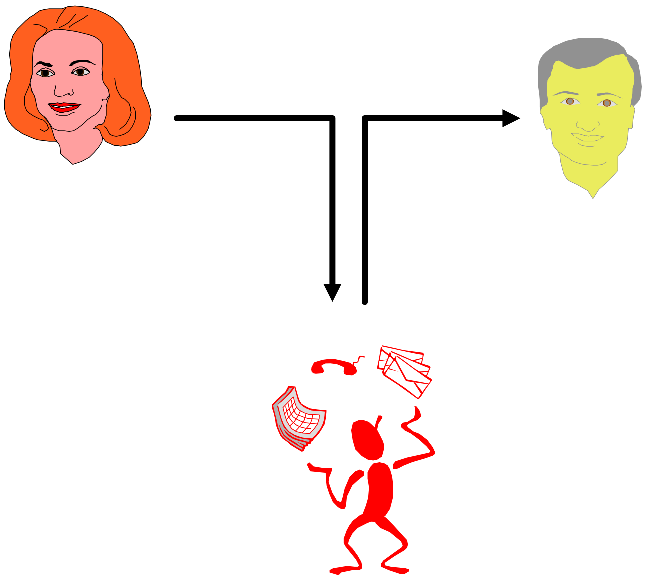


NANYANG TECHNOLOGICAL UNIVERSITY

Integrity

- Message is received as sent
- Modification
- Also interested in replay, re-ordering, deletion, delay

- **MODIFICATION**
  Gain access and "tampers" with messages

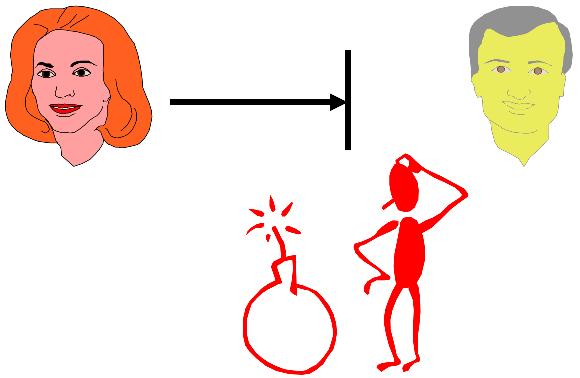


NANYANG TECHNOLOGICAL UNIVERSITY

Availability

- Complete loss of availability
- Reduction/Degradation in availability

- **INTERRUPTION**
  Loss of communication (cut the cable)
- **DENIAL OF SERVICE**
  Noisy comms (physical noise, spurious messages)

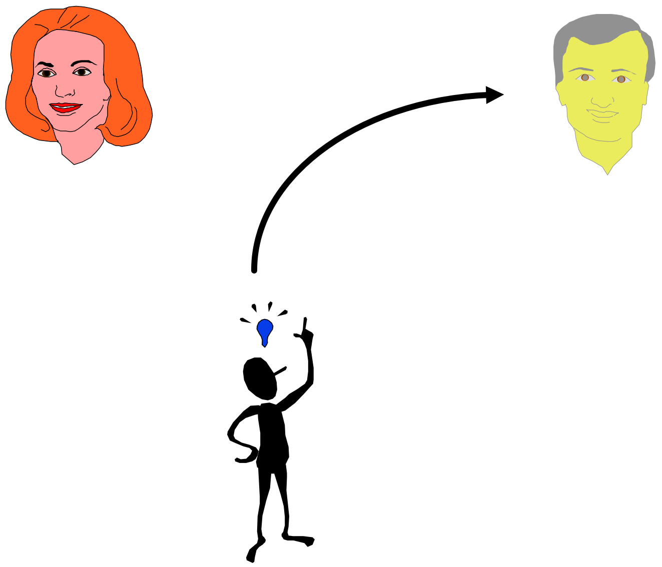


NANYANG TECHNOLOGICAL UNIVERSITY

Authentication

- Assurance that message is from proper source
- Protect from third party masquerade

- **FABRICATION**
  Insertion of “counterfeit” messages



Non-repudiation

- Prevents parties from denying they sent or received a message; i.e. concerned with protecting against legitimate protocol participants, not with protection from external source
- Receiver can verify **and prove** who sent a message
- Sender can verify **and prove** who received a message

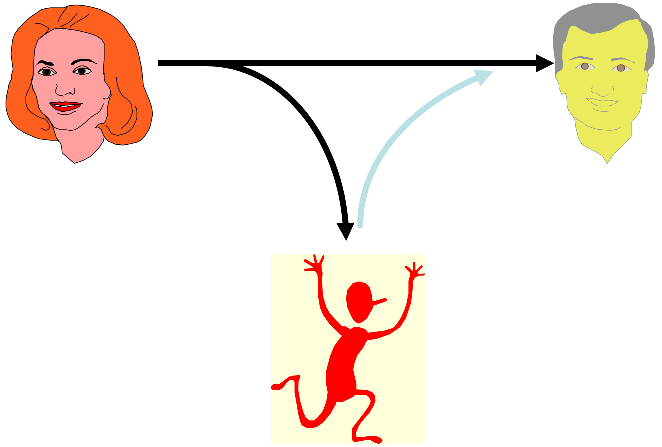
- **REPUDIATION ATTEMPT** Party anonymously publishes his or her message/key(s) and falsely claims that they were stolen.

NANYANG TECHNOLOGICAL UNIVERSITY

Privacy

- Limit and control access to host system/services
- Limit and control access to networks
- Authenticate each party so that access rights can be assigned
- More fine-grained solutions, e.g. Digital Rights Management

- **REPLAY**
  Record a legitimate message e.g. a login, and replay later



NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- Security Triad
- *Cryptographic Primitives*
    - ***Private-Key Cryptography***
    - Hash Function, Message Authentication Code
    - Public-Key Cryptography
    - Digital Signature
- Discussion

1 Go to wooclap.com
2 Enter the event code in the top banner

Event code
CPSSECURITY

NANYANG
TECHNOLOGICAL
UNIVERSITY

Kerckhoffs's Principle

- An encryption scheme should be secure even if enemy knows everything about it except the key
  - Attacker knows all algorithms
- Do not rely on secrecy of the algorithms ("security by obscurity")

SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war).

7th Century BC, Ancient Greece

Types of Symmetric-Key Cipher

- **Substitution Cipher**
  - A substitution cipher replaces one symbol with another.
  - Can be mono/poly-alphabetic

The following figures show two examples of a plaintext and its corresponding ciphertext. Which cipher is mono-alphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Plaintext: HELLO
Ciphertext: ABNZF

Types of Symmetric-Key Cipher *(contd.)*

- **Shift Cipher**
  - The shift cipher is also referred to as the Caesar cipher.

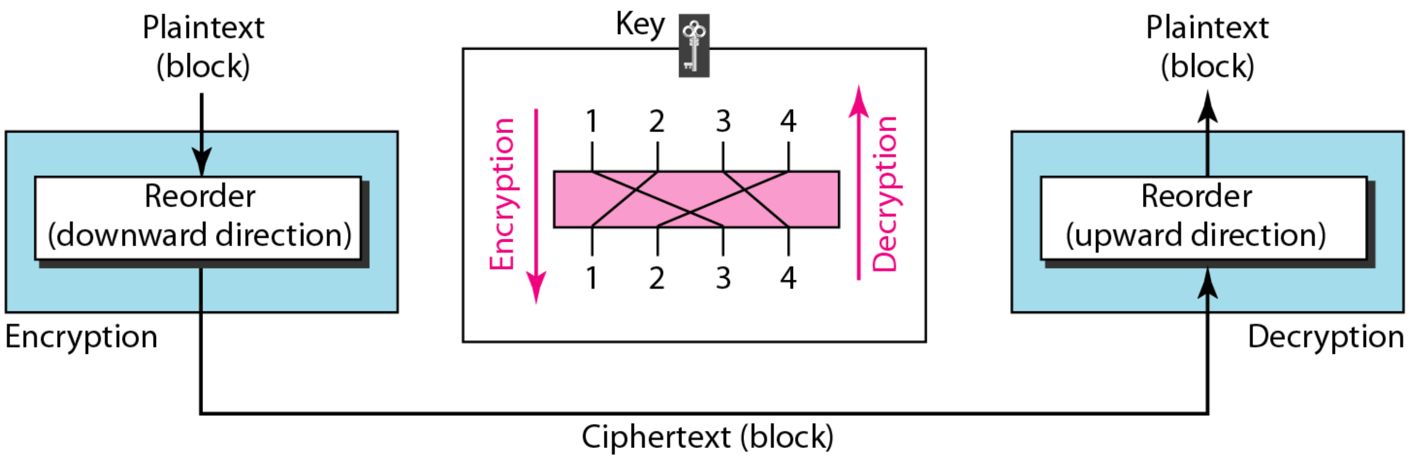
Use the shift cipher with key = 15 to encrypt the message “HELLO.”

Solution
We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

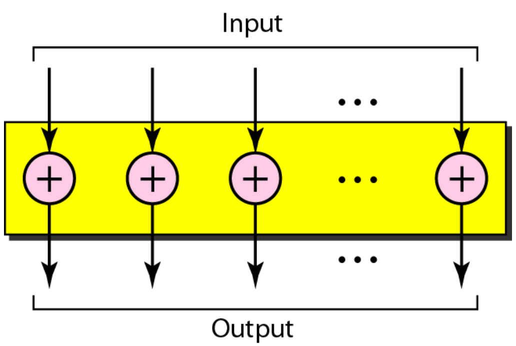
NANYANG TECHNOLOGICAL UNIVERSITY

Types of Symmetric-Key Cipher *(contd.)*

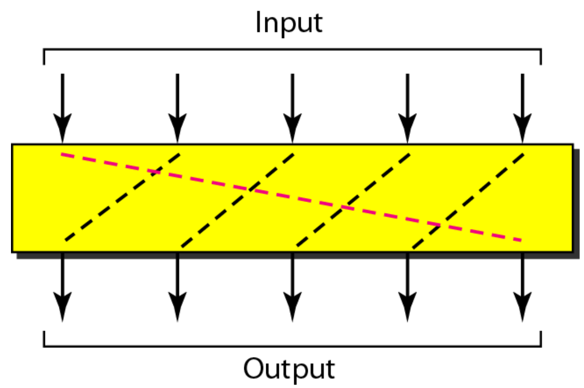
- **Transposition Cipher**
- A transposition cipher reorders (permutes) symbols in a block of symbols.



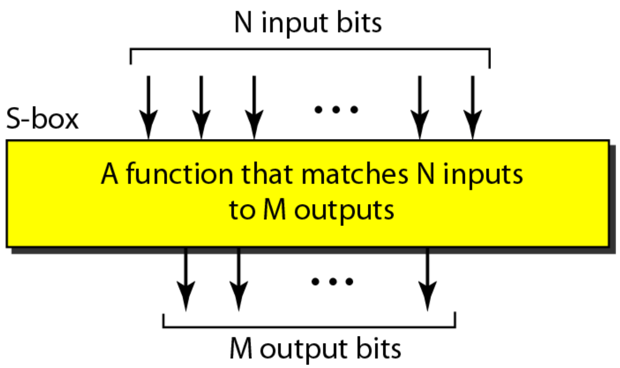
Components of Symmetric-Key Cipher



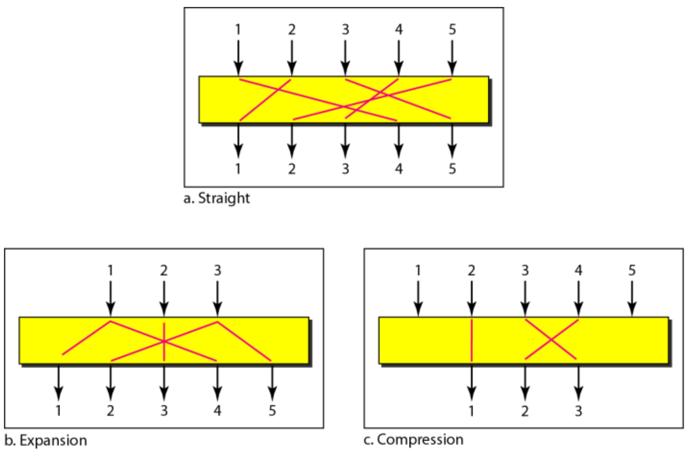
XOR substitution



Rotation substitution

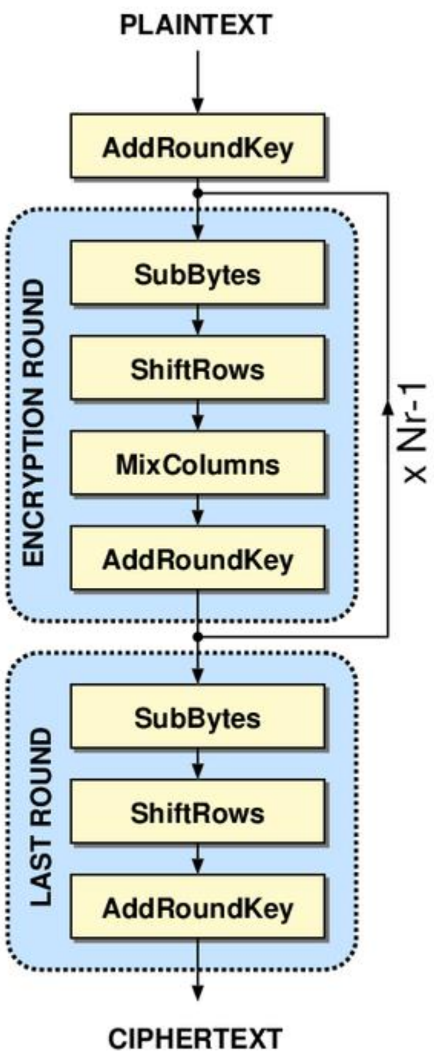


Substitution Box



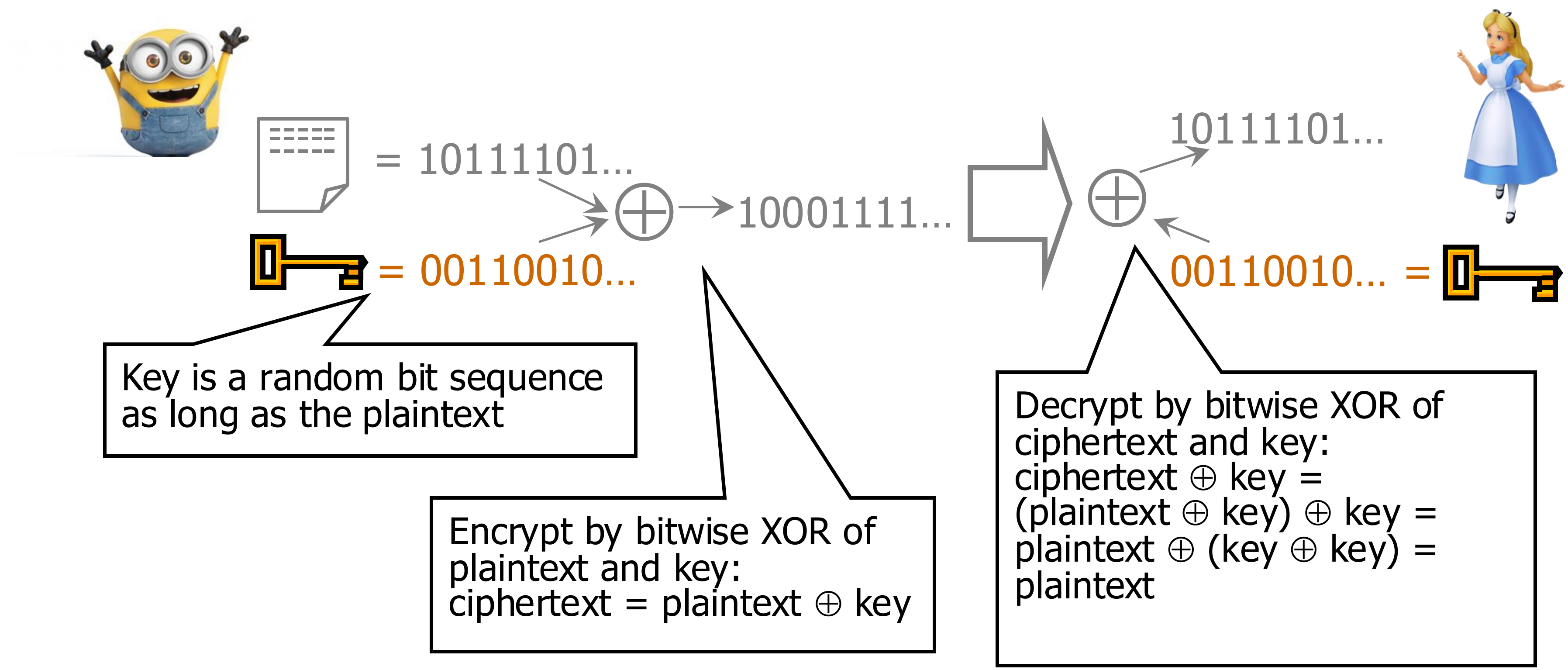
Permutation Box

Block Cipher: AES



NANYANG TECHNOLOGICAL UNIVERSITY

One-Time Pad (Vernam Cipher)

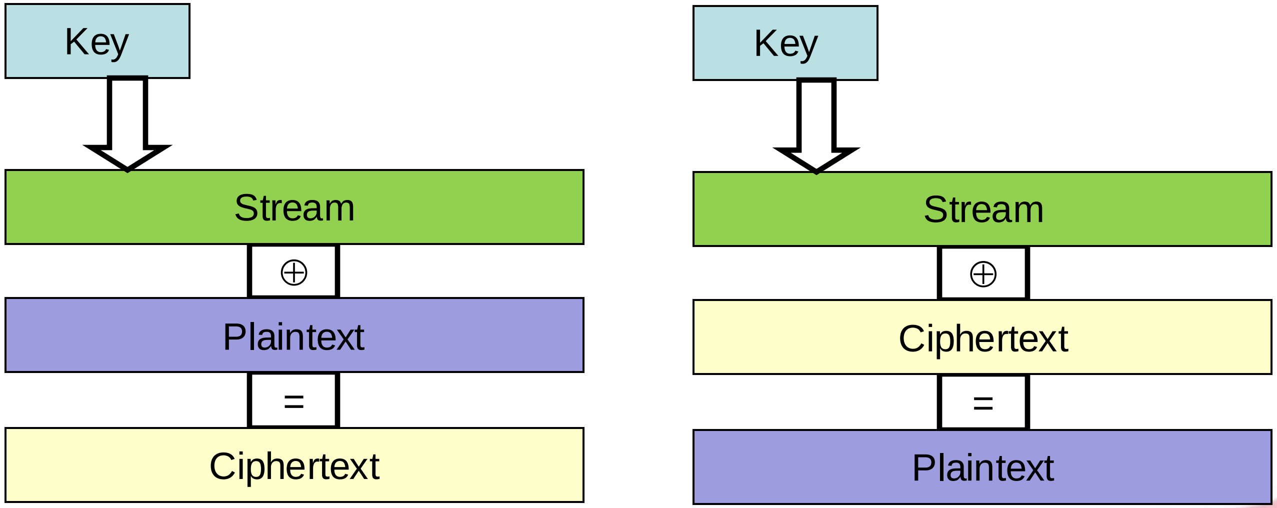


Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely *(Claude Shannon, 1949)*

NANYANG TECHNOLOGICAL UNIVERSITY

Stream Ciphers

- Start with a secret key ("seed")
- Generate a keying stream
  - Uses a Pseudo-Random Number Generator (PRNG)
- Combine the stream with the plaintext to produce the ciphertext (typically by XOR)



NANYANG TECHNOLOGICAL UNIVERSITY

Pseudo Random Number Generator

- Commonly constructed using Linear Feedback Shift Registers (LFSRs)
- An adversary cannot distinguish a PRNG output from a random sequence

- Example Randomness Tests
  - Monobit tests (frequency of 0s and 1s)
  - Run tests (frequency of runs of different lengths)
- *Pi: A naturally occurring random number*

String 1: 0101010101010101010101010101010101010101010101010101010101010101
String 2: 1100100001100001110111101110110011111010010000100101011110010110

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- Security Triad
- *Cryptographic Primitives*
  - Private-Key Cryptography
  - ***Hash Function, Message Authentication Code***
  - Public-Key Cryptography
  - Digital Signature
- Discussion

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

How to Authenticate Messages?

- content is authentic – bits are as sent
- sequence of messages is proper

Note: Separate problems

- confidentiality that the message is encrypted
- authenticity that the sender is genuine

Authenticating messages - Types

- Authenticator - a value that authenticates a message content
- Message Authentication Code, MAC (cryptographic checksum)
  - public function, with a given secret key produces fixed length value
- Hash or Message Digest
  - public function, which maps message (any length) to fixed-length hash value – no key

Message Authentication Code (MAC)

- Objective: assure authentic content
  - Message is not encrypted
- MAC is small fixed-size data block, appended to message M
- Generator and Validator share secret key

$$MAC_K[M] = F(M, key)$$

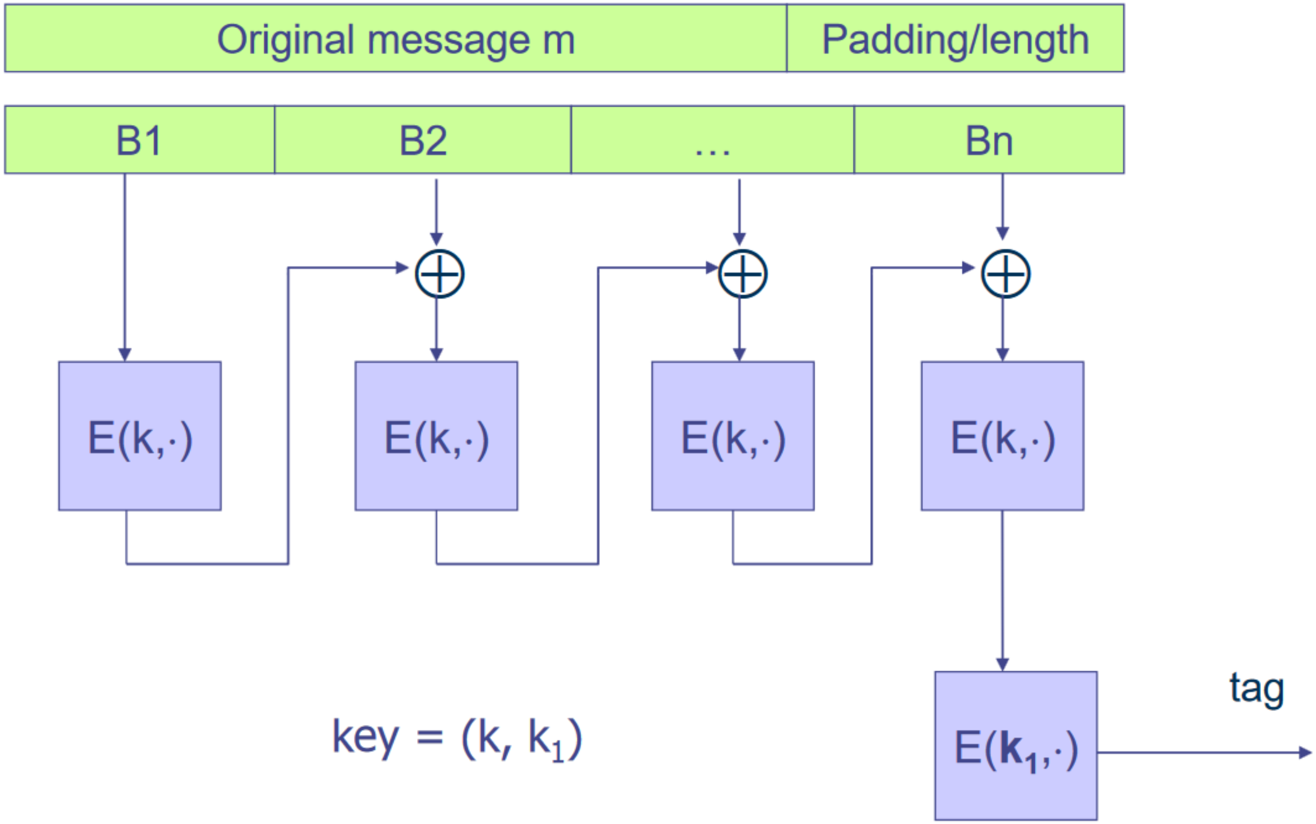
NANYANG TECHNOLOGICAL UNIVERSITY

Why use MAC, given encryption?

- Message may not need to be secret, but must be authentic
- Broadcast - only have one site responsible for monitoring authenticity. Broadcast plaintext plus MAC
- Overload - send plaintext messages (i.e. receiver need not decrypt). Authenticate selectively

NANYANG TECHNOLOGICAL UNIVERSITY

MAC Construction using Encryption



Cipher Block Chaining Message Authentication Code (CBC-MAC)

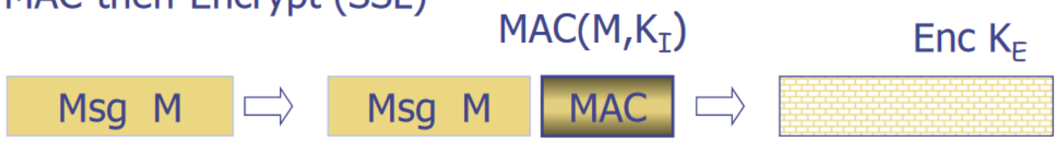
MAC usage

- message authentication (no confidentiality)
  - $A \rightarrow B$: $[M, MAC_K [M]]$
- authentication and confidentiality
  - $A \rightarrow B$: $E_{K1}[M, MAC_K [M]]$
- authentication and confidentiality
  - $A \rightarrow B$: $[E_{K1}[M], MAC_K [E_{K1}[M]]]$

MAC Usage *(contd.)*

Encryption key K_E MAC key = K_I

Option 1: MAC-then-Encrypt (SSL)



Option 2: Encrypt-then-MAC (IPsec)

Option 3: Encrypt-and-MAC (SSH)

NANYANG TECHNOLOGICAL UNIVERSITY

Hash function (Message Digest)

- no key
- like MAC, small amount of data; hash of message gives fixed-size value
- define hash function so that change of any one bit of message will result in different hash value
- hash function is not secret
- one-way; receiver re-computes hash function

NANYANG
TECHNOLOGICAL
UNIVERSITY

Simple Message Digest: Parity

- parity, or longitudinal redundancy check
- process one bit at a time
- use XOR

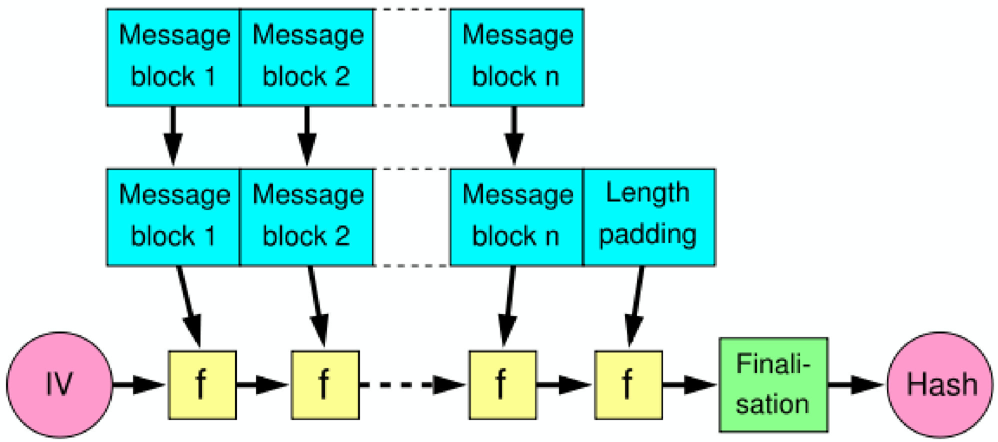
$$C = b_1 \oplus b_2 \oplus \cdots \oplus b_{n-1} \oplus b_n$$

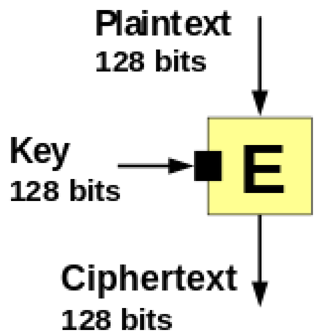
- input – arbitrary length message
- size of processed block – one bit
- output – one bit

NANYANG TECHNOLOGICAL UNIVERSITY

Merkle–Damgård Construction for Hash Functions

- Message is divided into fixed-size blocks and padded
- Use a one-way function f, which takes a chaining variable (of size of hash output) and a message block, and outputs the next chaining variable
- Final chaining variable is the hash value





f built out of block cipher

$$M = m_1 m_2 \ldots m_n;\ C_0 = IV, C_{i+1} = f(C_i, m_i);\ H(M) = C_n$$

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- Security Triad
- Cryptographic Primitives
- *Discussion*

1 Go to wooclap.com

2 Enter the event code in the top banner

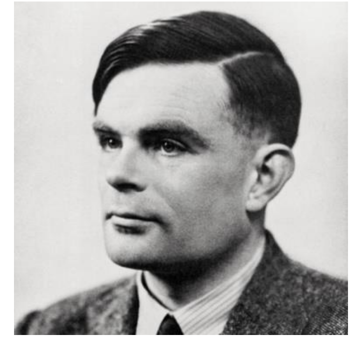
Event code

CPSSECURITY

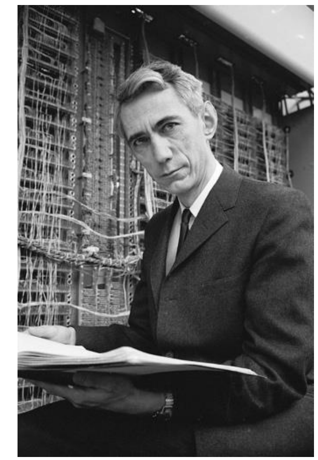
NANYANG TECHNOLOGICAL UNIVERSITY

What did we learn?

- **What is Security?**



  - Confidentiality, Integrity, Availability
  - *Authenticity, Privacy, Non-repudiation*



- **What are the building blocks of security?**
  - *Upcoming Lectures*
  - Private-Key Cryptography, Hash, MAC
  - Public-Key Cryptography, Digital Signature

NANYANG TECHNOLOGICAL UNIVERSITY

Further Reading

- Security Engineering
  – by Ross Anderson, available online - http://www.cl.cam.ac.uk/~rja14/book.html

- Handbook of Cryptography
  – by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, available online - http://cacr.uwaterloo.ca/hac/

- Applied Cryptography
  – by Dan Boneh and Victor Shoup, available online - http://toc.cryptobook.us/

- Leisure Reading - Simon Singh: *The Code Book*, Fourth Estate 1999

The End