Cryptography

CS 166: Introduction to Computer Systems Security
Security Goals?

Confidentiality
• Prevent disclosure of information to unauthorized parties

Integrity
• Detect data tampering

Availability
• Guarantee access to data

CIA Triad
Confidentiality
Integrity
Availability
Cryptography
Standard Communication

Sender

communication channel

Recipient

sent message

received message
Eavesdropping

Sender

Attacker

Recipient

sent message

read

received message

2/1/16

Cryptography
Tampering

sent message → modify → received message

Sender → Attacker → Recipient
Blocking

sent message

drop

received message

Sender

Attacker

Recipient

2/1/16

Cryptography
Attacks on Communication

• Eavesdropping
  • The adversary intercepts and reads the message (lack of confidentiality)

• Tampering
  • The adversary modifies the message (lack of integrity)

• Blocking
  • The adversary prevents the message from reaching the recipient (lack of availability)
Cryptography

• **Cryptography** provides methods for assuring the **confidentiality** and **integrity** of data that is
  – transmitted over communication channels (e.g., web pages and email messages)
  – stored on devices (e.g., files on a laptop or data center)

• We begin by explaining cryptographic concepts using the data transmission scenario
Encrypted Communication

plaintext → encrypt → ciphertext → decrypt → plaintext

Sender → encrypt → ciphertext → decrypt → plaintext → Recipient

Attacker: Cryptography
Encryption

• Encryption allows to secure communications
  – Originally focused on confidentiality alone

• Encryption combines the plaintext with an encryption key to produce the ciphertext
  – The ciphertext is transmitted instead of the plaintext

• Decryption combines the ciphertext with the decryption key to return the plaintext
  – Only the intended recipient should have the secret key

• Encryption and decryption should be computationally infeasible without the corresponding keys
CLASSIC CRYPTOGRAPHY
Classic Encryption Methods

• Used for military applications since ancient times
• Julius Caesar’s cipher
  – replace a with x
  – replace b with y …

• Alphabet shift cipher
  – Method: replace each character c of the plaintext with the character k positions after c in the alphabet
  – Key (for encryption and decryption): number k
  – Can be easily cracked by trying all possible values of k between 1 and the size of the alphabet
Substitution Cipher

• Arbitrary permutation of the characters
  – A \rightarrow K
  – B \rightarrow T
  – C \rightarrow G
  – ...

• The key is the sequence of permuted characters (KTG ...) 
• Number of possible keys for 26-character alphabet \( \approx 4 \times 10^{26} \) 
• Unfeasible to try all possible keys but ...
• Can be cracked by frequency analysis
  – most frequent letters in English: e, t, o, a, n, i, ...
  – most frequent digrams: th, in, er, re, an, ...
  – most frequent trigrams: the, ing, and, ion, ...
• Attack first described in a 9th century book by al-Kindi
Frequency Analysis (1)

Example

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCNPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPD. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?” OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK
Letter Frequencies Graph

First guess

- **LBO ➔** THE
Frequency Analysis (2)

PCQ VMJYPD THYK TYSE KHXHJXWXV HXV ZCJPE EYPD KHXHJYUXJ THJEE KCPK. CP THE THCMKXPV XPV IYJKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX'XJMI, KHE JCKE XPV EYKKEV THE DJCMPV ZEICJE HYS, KXUYPD: “DJEXT EYPD, ICJ X THCMKXPV XPV CPE PYDHTK Y HXNE ZEEP JEACMPTYPD TC UCM THE IXZREK CI FXKT XDEK XPV THE REDEPK CI XPAYEPT EYPD. SXU Y SXEE KC ZCRV XK TC AJXNE X IXNCMJ CI UCMJ SXGEKTU?”

More guesses

- J ➔ ...
  ... R
- K ➔ ...
  ... S
- X ➔ ...
  ... A or I
To experiment with classic cryptography, visit [www.cryptoclub.org](http://www.cryptoclub.org)

### Frequency Analysis (3)

| PCQ VMJYPD LBYK LYSO | Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: “great king, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”  

Epilogue, Tales from the Thousand and One Nights |
| KBXBJXWV BXV ZCJPO EYPD | OFYRCDMO, LXROK IJCS LBO |
| KBXBXYUXJ LBJO0 KCPK, CP LBO | LBCMKXPV XPV CPO PYDBLK |
| LBCMKXVP XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXVP XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?“ |

2/1/16

Cryptography
MODERN CRYPTOGRAPHY
Requirements of Modern Cryptography

Before Computer Age (~1950)

• Kerckhoff’s Principle (1883)
  security based on key only, adversary knows cryptographic method
  aka “no security by obscurity”

• Simple, light crypto machines
• Rugged for military use
• Adversary has access to some plaintext/ciphertext pairs

Now (added requirements)

• Hardware/software implementation
• Resistant to huge amount of computing power
• Random number generators
• Adversary has access to unlimited ciphertext and lots of chosen plaintext/ciphertext pairs
Symmetric Key Cryptography

- Same key used for encryption and decryption
- Encryption and decryption algorithms are one the reverse of the other
Symmetric Key Cryptography

• Advantages
  – Conceptual simplicity
  – Suitable for one-to-one communication (e.g. confidential email)

• Disadvantages
  – Setup requires secure channel to exchange key
  – Unsuitable for many-to-many communication (e.g. sharing secure data)
Modern Symmetric Cryptography

Data Encryption Standard (DES)
• Developed by IBM in collaboration with the NSA
• Became US government standard in 1977
• 56-bit keys
• Exhaustive search attack feasible since late 90s

Advanced Encryption Standard (AES)
• Selected as US government standard in 2001 through open competition
• 128-, 192-, or 256-bit keys
• Exhaustive search attack not currently possible
Public Key Cryptography

- **RSA**: Most widely used public key cryptosystem today
- Invented by Rivest, Shamir, and Adleman (1978)
- Clifford Cocks and Jame Ellis developed equivalent system in 1973 classified by UK until 1997
- Patent expired in 2000
- 2048-bit (or longer) keys recommended
- Much slower than AES
- Typically used to encrypt an AES symmetric key
Non-Secret Encryption

- Lock and unlock are inverse operations
- Alice can:
  - Buy a lock
  - Keep the key
  - Send the lock to Bob
- Bob can:
  - Lock his message with Alice lock
  - Send back the lock to Alice
- Alice can open the lock
- NO KEYS ARE EXCHANGED
- Alice can publish the lock and let anyone to use send her a message

2/1/16 Cryptography
Public Key Cryptography

Key pair
• **Public key**: shared with everyone
• **Secret key**: kept secret, hard to derive from the public key

Protocol
• Sender encrypts using recipient's public key
• Recipient decrypts using its secret key

Sender
public key
encrypt
plaintext
ciphertext
decrypt
plaintext
Recipient
secret key
Attacker
Cryptography
Public Key Cryptography

- Advantages
  - A single public-secret key pair allows receiving confidential messages from multiple parties

- Disadvantages
  - Conceptually complex
  - Computationally expensive
Is Crypto Secure Enough?

Cryptographic Module Validation Program

• Managed by
  – Communications Security Establishment (CSE) Canada
  – National Institute of Standards and Technology (NIST) USA

• Validates cryptographic modules against
  – Federal Information Processing Standard (FIPS) 140-1 and FIPS 140-2
  – Other cryptography based standards
CRYPTO INTRO
Crypto Intro

• Encryption and Decryption
• Symmetric systems use the same key
• Asymmetric systems use different keys
  – A pair public/private

Security coordinate
1. Confidentiality
2. Integrity
3. Availability

A general attack
1. Eavesdropping
2. Tampering
3. Blocking