COMS3000/7003

Week 8

Introduction to Cryptography,
Symmetric Cryptography

Assignment

- DUE 4:00 pm FRIDAY 22 September 2017

Submission Instructions

The following items need to be submitted:

- A hard-copy of the assignment is to be submitted through the Faculty of EAIT (Hawken Building 50) assignment chute and requires a **signed assignment cover sheet**.
- You also need to submit an **electronic version** of your assignment in PDF format via Blackboard.

The submission deadline is 4:00 pm Friday 22/9/17 – both copies must be submitted. The hardcopy will be returned to you before the revision period at the end of semester.

Good time management is critical. Students should not expect any significant assistance from the lecturer or tutor on this assignment in the last few days before the deadline.

- I will be on overseas business from Wednesday and will not have routine access to email – see Dr Kaleb Leemaqz <k.leemaqz@uq.edu.au>

Assignment

- NO LECTURE NEXT WEEK – submit your assignment by 4:00 pm – I recommend you submit your assignment before the assignment centre staff leave at 2:00 pm
- NO tutorial questions next week - last chance for any last minute assignment questions with Dr Leemaqz in the tutorials
- In addition, I will hold an open assignment consultation session here after this lecture

Assignment

- Tutors cannot review 125 drafts.
- You can ask the tutors any questions about the assignments during the tutorials.
- The libraries provide expert help on style, research sources, citation and referencing.

Reminder: Late Assessments

- **See course profile**: As given in the first lecture:
- "The submission of progressive assessment material on the due date as set out in this Electronic Course Profile is the sole responsibility of the student."
- "Unless advised in the Course Profile, assessment items received after the due date will receive a zero mark unless you have been approved to submit the assessment item after the due date.
- However, if there are medical or exceptional circumstances that will affect your ability to complete an assessment by the due date, then you can apply for an extension via the following methods:"

“5.3 Late Submission” (ECP)

- “You can find further information and the relevant forms online. The ***Application for Extension of Assessment Due Date*** form and supporting documentation (e.g. medical certificate) can be submitted by email to *enquiries@itee.uq.edu.au* or in person to the School office (General Purpose South [78], level 4 Coursework Studies Office).”

“5.3 Late Submission” (ECP)

- Requests must be made at least 48 hours prior to the submission deadline, unless the medical or other circumstances are such that you could not reasonably be expected to have applied by then.”
- “Requests for extensions which are received on or after the due date may not be able to be considered.

- The School will issue a notification of the outcome to your student email account.”

“5.3 Late Submission” (ECP)

- For assignments that require both a hard copy as well as an electronic submission, the assignment is considered as submitted only when BOTH the hard copy AND the electronic version have been submitted. If the two versions are submitted at a different time or day, the later submission time and day will be considered.”

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Modern password crackers combine different words from their dictionaries:

> What was remarkable about all three cracking sessions were the types of plains that got revealed. They included passcodes such as "k1araj0hns0n," "Sh1a-labe0uf," "Apr!l221973," "Qbesancon321," "DG091101%," "@Yourmom69," "ilovetofunot," "windermere2313," "tmdmmj17," and "BandGeek2014." Also included in the list: "all of the lights" (yes, spaces are allowed on many sites), "i hate hackers," "allineedislove," "ilovemySister31," "iloveyousomuch," "Philippians4:13," "Philippians4:6-7," and "qeadzcwrsfxv1331." "gonefishing1125" was another password Steube saw appear on his computer screen. Seconds after it was cracked, he noted, "You won't ever find it using brute force."

This is why the oft-cited XKCD scheme for generating passwords -- string together individual words like "correcthorsebatterystaple" -- is no longer good advice. The password crackers are on to this trick.

That was re-posted from 2013

- **A Really Good Article on How Easy it Is to Crack Passwords** (from Lecture 3)
- https://www.schneier.com/blog/archives/2013/06/a_really_good_a.html

- This was: **Choosing Secure Passwords**
- https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

Industry Certifications

Topics we have touched on so far…

(ISC)²® CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering (Physical Security)**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

(ISC)²® CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering (Physical + Crypto)**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

ISACA® CISM® Domains

- The ISACA Certified Information Security Manager credential covers 4 job practice domains:
- **Information Security Governance (24%)**
- **Information Risk Management (30%)**
- **Information Security Program Development and Management (27%)**
- **Information Security Incident Management (19%)**

ISACA® CISM® Domains

➢ Information Security Governance (24%)

Task Statements

1.1 Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

1.2 Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.

1.4 Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

1.5 Develop business cases to support investments in information security.

1.6 Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.

1.7 Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

1.8 Define, communicate, and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.

1.9 Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

Knowledge Statements

k1.1 Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research)

k1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices

k1.3 Knowledge of available information security governance frameworks

k1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development

k1.5 Knowledge of the fundamental concepts of governance and how they relate to information security

k1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework

k1.7 Knowledge of methods to integrate information security governance into corporate governance

k1.8 Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development

k1.9 Knowledge of content in, and techniques to develop, business cases

k1.10 Knowledge of strategic budgetary planning and reporting methods

k1.11 Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy

k1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)

k1.13 Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security)

k1.14 Knowledge of roles and responsibilities of the information security manager

k1.15 Knowledge of organizational structures, lines of authority and escalation points

k1.16 Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users)

k1.17 Knowledge of processes to monitor performance of information security responsibilities

k1.18 Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization

k1.19 Knowledge of methods to select, implement and interpret key information security metrics (e.g., key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])

Information Security Governance

- More on Governance after the mid-semester break

ISACA® CISA® Domains

- The ISACA Certified Information Security Auditor credential covers 5 job practice domains:
- **The Process of Auditing Information Systems (21%)**
- **Governance and Management of IT (16%)**
- **Information Systems Acquisition, Development and Implementation (18%)**
- **Information Systems Operations, Maintenance and Service Management (20%)**
- **Protection of Information Assets (25%)**

ISACA® CISA® Domains

- **Governance and Management of IT (16%)**
- **Task 2.7 Evaluate risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.**
- **Knowledge 2.11 Knowledge of enterprise risk management (ERM)**

ISACA® CISA® Domains

➢ Protection of Information Assets (25%)

Task Statements:

5.1 Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.

5.2 Evaluate the design, implementation, maintenance, monitoring and reporting of physical and environmental controls to determine whether information assets are adequately safeguarded.

5.3 Evaluate the design, implementation, maintenance, monitoring and reporting of system and logical security controls to verify the confidentiality, integrity and availability of information.

5.4 Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.

5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of assets to determine whether information assets are adequately safeguarded.

5.6 Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.

Knowledge Statements:

5.1 Knowledge of the generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets

5.2 Knowledge of privacy principles

5.3 Knowledge of the techniques for the design, implementation, maintenance, monitoring and reporting of security controls

5.4 Knowledge of the physical and environmental controls and supporting practices related to the protection of information assets

5.5 Knowledge of the physical access controls for the identification, authentication and restriction of users to authorized facilities and hardware

5.6 Knowledge of the logical access controls for the identification, authentication and restriction of users to authorized functions and data

5.7 Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems) and database management systems.

5.8 Knowledge of the risk and controls associated with virtualization of systems

5.9 Knowledge of the risk and controls associated with the use of mobile and wireless devices, including personally owned devices (bring your own device [BYOD])

5.10 Knowledge of voice communications security (e.g., PBX, Voice-over Internet Protocol [VoIP])

5.11 Knowledge of network and Internet security devices, protocols and techniques

5.12 Knowledge of the configuration, implementation, operation and maintenance of network security controls

5.13 Knowledge of encryption-related techniques and their uses

5.14 Knowledge of public key infrastructure (PKI) components and digital signature techniques

5.15 Knowledge of the risk and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs, cloud computing)

5.16 Knowledge of the data classification standards related to the protection of information assets

5.17 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

5.18 Knowledge of the risk and controls associated with data leakage

5.19 Knowledge of the security risk and controls related to end-user computing

5.20 Knowledge of methods for implementing a security awareness program

5.21 Knowledge of information system attack methods and techniques

5.22 Knowledge of prevention and detection tools and control techniques

5.23 Knowledge of security testing techniques (e.g., penetration testing, vulnerability scanning)

5.24 Knowledge of the processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

5.25 Knowledge of the processes followed in forensics investigation and procedures in collection and preservation of the data and evidence (i.e., chain of custody).

5.26 Knowledge of the fraud risk factors related to the protection of information assets

PCI Data Security Standard

Six Goals, Twelve Requirements

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI Data Security Standard

- Build and Maintain a Secure Network
  - 1. Install and maintain a firewall configuration to protect cardholder data
  - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - 3. Protect stored cardholder data
  - 4. Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - 5. Use and regularly update anti-virus software or programs
  - 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - 7. Restrict access to cardholder data by business need-to-know
  - 8. Assign a unique ID to each person with computer access
  - 9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - 10. Track and monitor all access to network resources and cardholder data
  - 11. Regularly test security systems and processes
- Maintain an Information Security Policy
  - 12. Maintain a policy that addresses information security for employees and contractors

PCI Data Security Standard

- Build and Maintain a Secure Network
  - 1. Install and maintain a firewall configuration to protect cardholder data
  - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - 3. Protect stored cardholder data
  - 4. Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - 5. Use and regularly update anti-virus software or programs
  - 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - 7. Restrict access to cardholder data by business need-to-know
  - 8. Assign a unique ID to each person with computer access
  - 9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - 10. Track and monitor all access to network resources and cardholder data
  - 11. Regularly test security systems and processes
- Maintain an Information Security Policy
  - 12. Maintain a policy that addresses information security for employees and contractors

Any questions so far?

Continuing on with…
Cryptography

Basic Model - Terminology

Sender
(Alice)

Recipient
(Bob)

Plaintext
(cleartext)

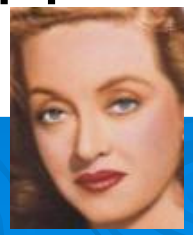
Encryption
Algorithm
(cipher)

Ciphertext

Decryption
algorithm

Original
Plaintext

Eavesdropper
(Eve)



Cryptographic Algorithms (Ciphers)

- We have to ensure that only legitimate or authorised users are able to (encrypt and) decrypt
- A simple way to do this is to restrict knowledge of the algorithms to authorised individuals.
  - **Keep Encryption/Decryption algorithm secret**

- **Problem ?**
  - This would mean that for every different set of people who wanted to communicate, there would have to be a different algorithm.
  - It becomes very impractical to keep using different algorithms – it is rather difficult to invent new ones which are resistant to cryptanalysis.
  - If an encryption algorithm gets in the hand of an attacker, we need to invent a new algorithm.

  - What is a better approach?

Cryptographic Keys

- Modern algorithms are actually large classes of encryption and decryption functions
- The sender and receiver need to use the corresponding functions
- The “index” of the function is called the **key**
  - The function is parameterised by the key

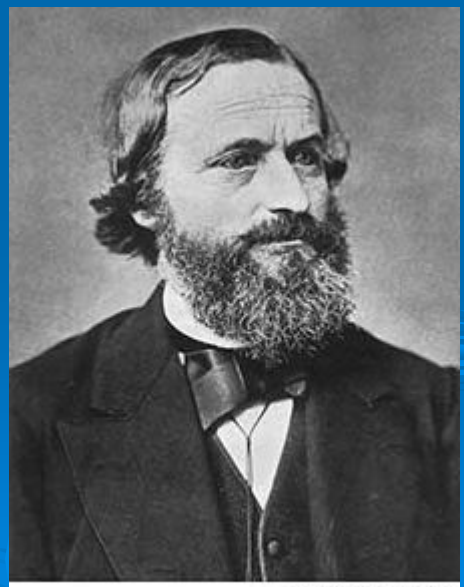
- For **symmetric** encryption algorithms the same key is used for encryption and decryption.
  - If Alice uses encryption function (key) 17, then Bob has to use decryption function (key) 17.
- Rather than having to keep the algorithms themselves secret, the security rests in the secrecy of the key.

- We have traded off one difficulty for another
  - Previously: needed to develop many new algorithms, and keep them secret
  - Now: We only need to distribute keys and keep them secret

Kerckhoffs' Principle

Auguste Kerckhoffs
(cryptography)

NOT Gustav Kirchhoff
"Kirchhoff's Laws"
(radiation)



Kerckhoffs' Principle

The security of a cipher should rely on the secrecy of the key only!

Auguste Kerckhoffs, "La Cryptographie militaire", 1883

- Assumption: Attacker knows every detail of the cryptographic algorithm
- Rationale:
  - Shannon used the expression: „The enemy knows the system“.
  - A determined attacker is generally able to to obtain a blueprint of an encryption/decription algorithm anyway, by clever decuction, stealing etc.
  - Cryptographic history has demonstrated this many times over.
- Alternative:
  - “Security through Obscurity“
    - Considered bad practice
  - Security relies on keeping the design of a system secret.
  - Example:
    - Storing house key under the door mat
  - Obscure codes, ciphers, and crypto systems have repeatedly fallen to attack regardless of the obscurity of their design and vulnerabilities
    - Example: **A5/1** cipher used for GSM mobile phones
    - Initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weakness in the cipher have been identified.

Improved Basic Model

Sender
(Alice)

encryption key
K_e

Recipient
(Bob)

decryption key
K_d

Plaintext
(cleartext)

Encryption
Algorithm
(cipher)

Ciphertext

Decryption
algorithm

Original
Plaintext

Eavesdropper
(Eve)

Cryptographic Algorithms (Ciphers)

So now we have: $C = E_{Ke}(P)$ and $P = D_{Kd}(C)$

Identity: $P = D_{Kd}(E_{Ke}(P))$

- Some algorithms use the *same* key for encryption as well as decryption, i.e. $K_e = K_d$
  - These are called **symmetric algorithms** or **secret-key** algorithms
  - Mechanical Analogue:

- Other ciphers use a different key for encryption and decryption, i.e. $K_e \neq K_d$
  - These are called **asymmetric algorithms** or **public-key ciphers** and we will look at them later.

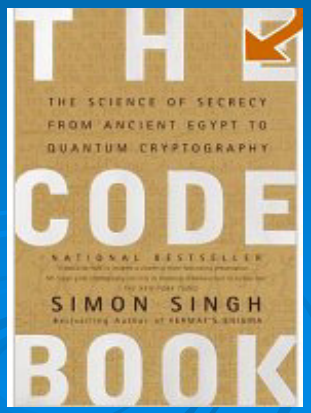
Terminology (again)

- Cryptography
  - Literally “secret writing”
  - Science & art (practice) of keeping messages secure
- Cryptanalysis
  - Science & art (practice) of breaking message security
- Cryptology
  - “Secret words” Science of secret communications (theory and mathematics) associated with cryptography and cryptanalysis

Famous Victim of Successful Cryptanalysis

Mary Stuart
(1516 - 1558)
Queen of Scotland

Elizabeth I
Queen of England



Codes have decided the fates of empires throughout recorded history

Mary Stuart, Queen of Scotland was put to death by her cousin Queen Elizabeth of England, for the high crime of treason after spymaster Sir Francis Walsingham cracked the secret code she used to communicate with her conspirators.

Source: Simon Singh, „The Code Book“, Doubleday, 1999

Types of Attacks

- Goal of attacker:
  - recover the plaintext, or even better, deduce the key
- Classification according to information available to an attacker
  - Ciphertext only attack
    - Attacker knows ciphertext of several messages encrypted with the same key and/or several keys
  - Known-Plaintext Attack
    - Known ciphertext / plaintext pair of several messages
  - Chosen-Plaintext Attack
    - Attacker can choose the plaintext that gets encrypted thereby potentially getting more information about the key
  - Adaptive Chosen-Plaintext Attack
    - Attacker can choose a series of plaintexts, basing the choice on the result of previous encryption → "differential cryptanalysis"
- Brute force attack:
  - Try every possible key
  - → If this is the best an attacker can do against a cipher, it is considered secure or strong
  - Security can be adjusted by choosing key length

Any questions so far?

How can you encrypt a message?

- Imagine you want to send the following secret message to someone
  - “attack at dawn”
- What type of cipher could you use?
- You don’t have a computer, just pen and paper.

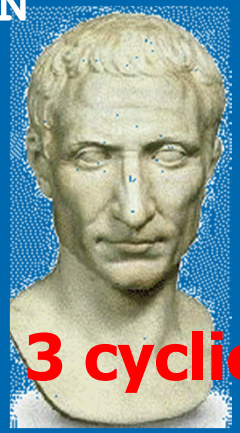
Caesar Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN

Substitution Table - Caesar's Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC ← key = 3 cyclic shifts



PHVVD JHIUR PPDUB VWXDU WNLOO WKHTX HHQ

The Caesar Cipher is an example of a **substitution cipher**.
→ one letter is replaced by another
The Caesar Cipher uses a shift of **3** positions of the alphabet
We can generalise this and use any shift k, for 0< k <26
How secure is this cipher?
Not secure at all.
There are only 25 different keys. → Brute force attack is easy

How can we make this cipher stronger?

Monoalphabetic Substitution Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN

General Substitution Table

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EYUOBMDXVTHIJPRCNAKQLSGZFW ← ? possible keys

JBKKE DBMAR JJEAF KQLEA QHVII QXBNL BBP

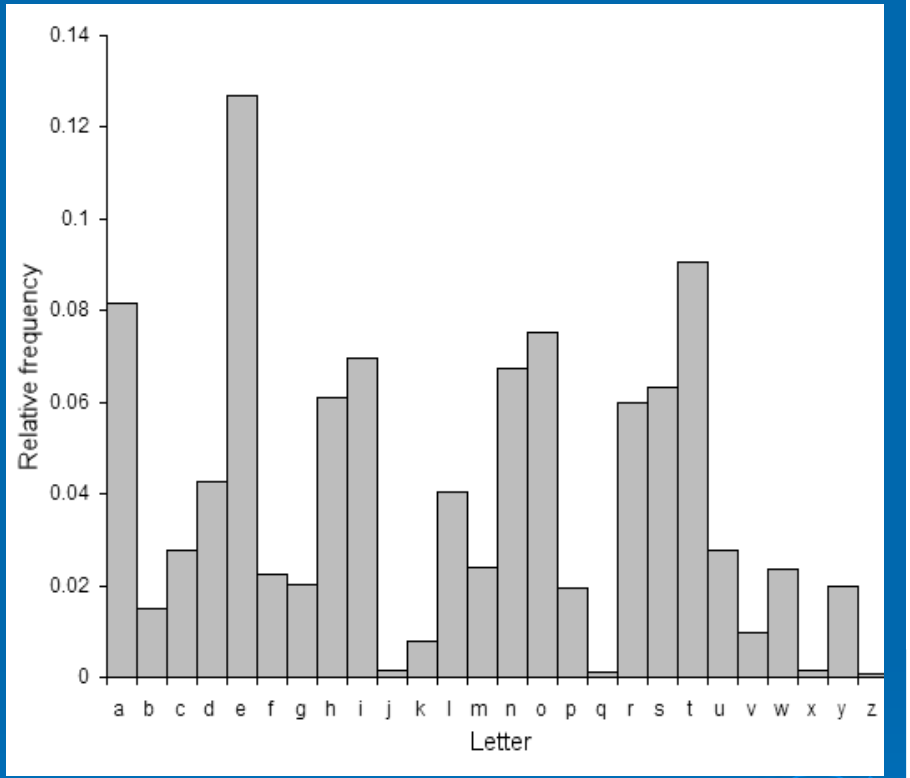
- The Ceasar cipher is an example of a monoalphabetic substitution cipher
- Instead of just shifting the alphabet, we use any permutation
- How many possibilities?
  - Permutation of 26 letters
  - → 26! ≈ 4* 10^{26} possible keys
- Is a monoalphabetic substitution cipher secure?
  - Brute force attack?
    - If we can test 1 Billion keys per second it will still take more than a 10 Billion years on average to find the key!!
      Very large “key space”, secure against brute force attack
  - Is there a better attack?

Frequency Analysis

Better approach: use **statistics**

- Relative frequency of letters in the English language

- Since each letter is replaced with another one, the statistics don't change
- The most frequent letter in the ciphertext corresponds most probably to an ***e*** in the plaintext
- The second most frequent letter corresponds to the letter ***t,*** and so forth..
- Can also use statistics of N-grams
  - Common digrams: th, in, er, re, an
  - Common trigrams: the, ing, and, ion
- This is called **Frequency Analysis**
- It is a bit like solving a cross-word puzzle
  - http://en.wikipedia.org/wiki/Frequency_analysis

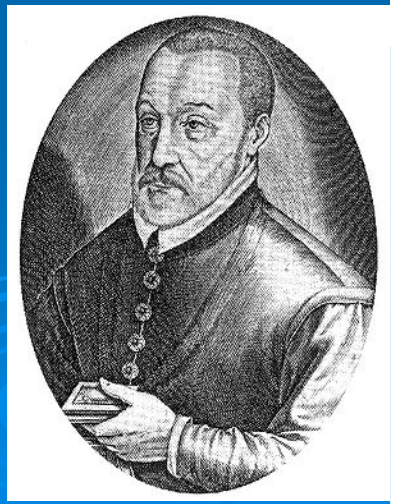


- Monoalphabetic substitution ciphers can be broken very easily with frequency analysis
  - → A large key space alone is does no guarantee for security of a cipher!!

Vigenère Cipher

- Even though monoalphabetic substitution ciphers are resistant to brute force attack, they can easily be broken with frequency analysis
- How can we extend the substitution cipher so that it is more resistant to frequency analysis?
- Use multiple alphabets
  - Use a different alphabet (key) for each letter
  - → "Polyalphabetic cipher"
  - → the same letter is mapped to different ciphertext letters
    - Frequency distribution of plaintext and ciphertext are now different

- Vigenère Cipher
  - Attributed to Blaise de Vigenère, a French diplomat
  - Actually invented by Giovan Battista Bellaso 1553
  - Thought to be unbreakable for a very long time (>250 years)
    - "Le chiffre indéchiffrable "
  - Combination of 26 different Caesar ciphers
    - → Vigenère square
    - → each row corresponds to a Caesar cipher



Vigenère Polyalphabetic Substitution Cipher

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

← Vigenère square

Keyword: **WHITE**

MESSAGE: **ATTACKATDAWN**
Key: **WHITEWHITEWH**

Ciphertext: **WABTGGHBWESU**

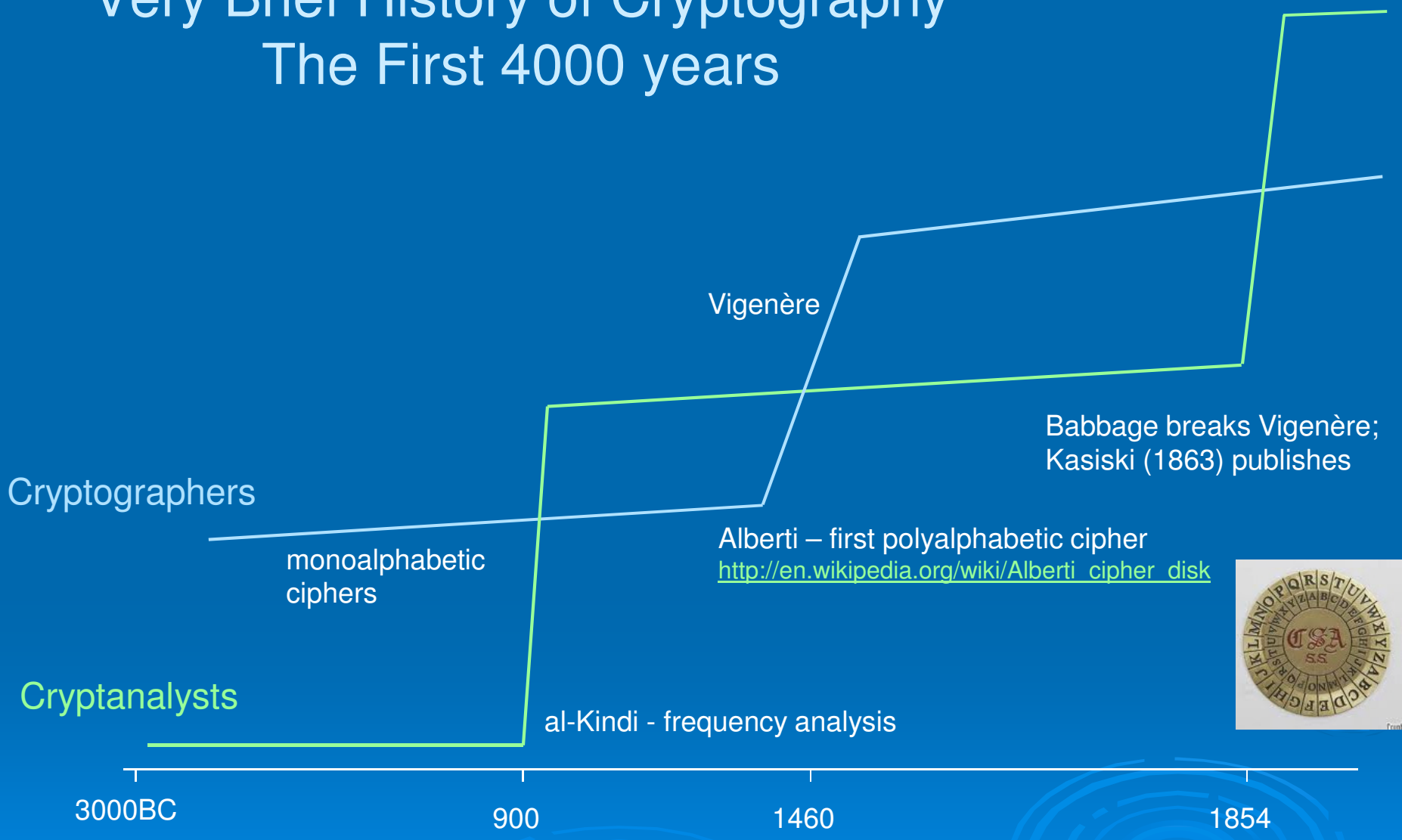
Breaking the Vigenère Cipher

- Look for repeated words (N-grams) in ciphertext, with N > 2
- How can these repetitions happen?
  - By coincidence, small probability for longer words
  - Same plaintext word is encrypted with the same key
    - Key lines up with same plaintext word
- `Message:  TheSpiesLeftTheCountry`
- `Key:ABC  ABCABCABCABCABCABCABCA`
- `Ciphertext: TIGSQLETNEGVTIGCPWNUTY`
- `Ciphertext: TIGSQLETNEGVTIGCPWNUTY`
- Determine key length ***n***
  - In a Vigenère cipher with key length ***n,*** every *n*-th letter is encrypted with the same Caesar cipher
  - Can use frequency analysis to break the ***n*** Caesar ciphers individually
- How can we determine the key length?
  - Repetitions must have a distance that is a multiple of the key length
  - In the above example, the distance is 12
  - Possible key lengths:
    Factors of distance 1,2,3,4,6,12

“Kasiski Test”

- First invented by Charles Babbage
- Later independently invented by **Friedrich Wilhelm Kasiski**
  - Find repetitions of N-grams, N > 2
  - Write down distances of repetitions
  - Key length is likely to be the gcd (greatest common divisor) of these distances
- Example:
  - The word ‘MHL’ is repeated at distances 72, 21, 24
  - What’s a likely key word length?
  - Factors of distances:
    - 24: 1,2,3,4,6,12,24
    - 21: 1,3,7,21
    - 72: 1,2,3,4,6,8,9,12,18,24,36,72
  - Likely key word length?
    - → 3

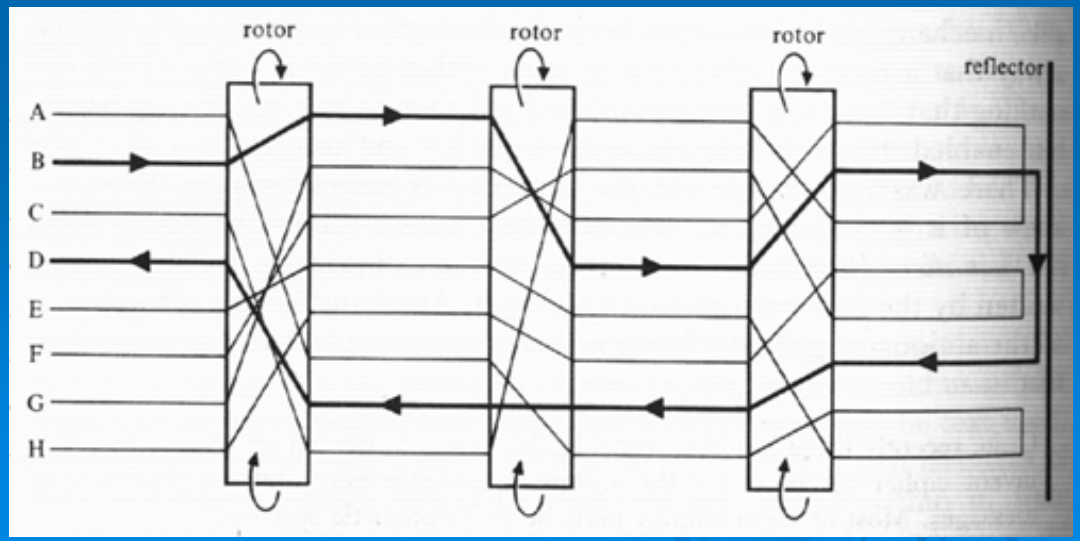
Very Brief History of Cryptography
The First 4000 years

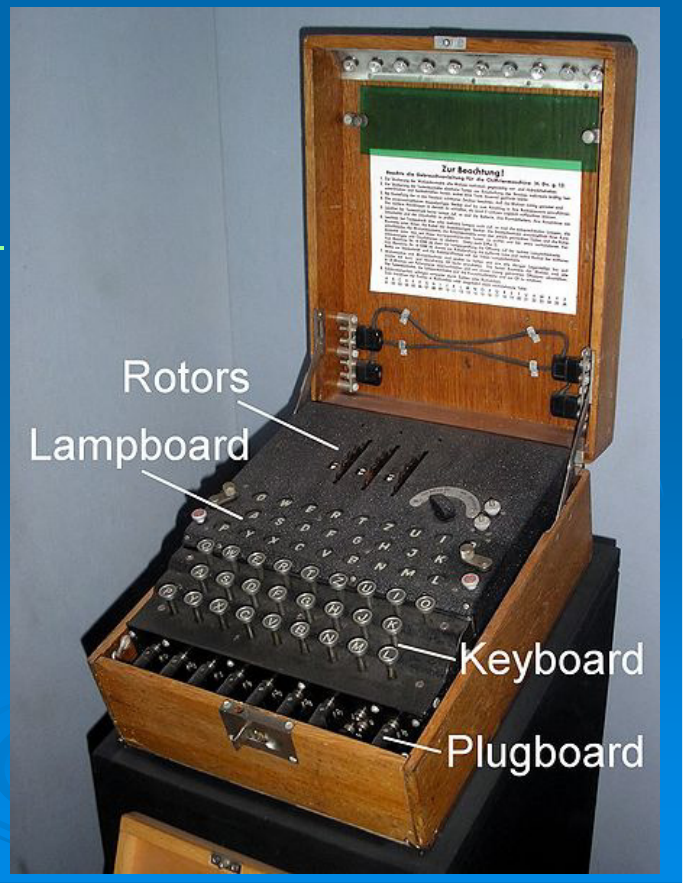


Source: David Evans, University of Virginia, Course CS588

Enigma Cipher

- Famous example of a polyalphabetic substitution cipher
  - Key space (rotor settings, plug board settings, …): ~180 * 10^{18}
- First broken by the Polish Cipher Bureau, before WWII
- Enhanced and used in WWII by Germany
- Broken by British, with help of Polish cryptologic bomb
  - Bletchley Park (Alan Touring)
- http://en.wikipedia.org/wiki/Enigma_machine
- http://www.youtube.com/watch?v=EJArtganaQQ
- https://www.youtube.com/watch?v=Hb44bGY2KdU





Movies on Enigma

- “The imitation game”
- “Enigma”

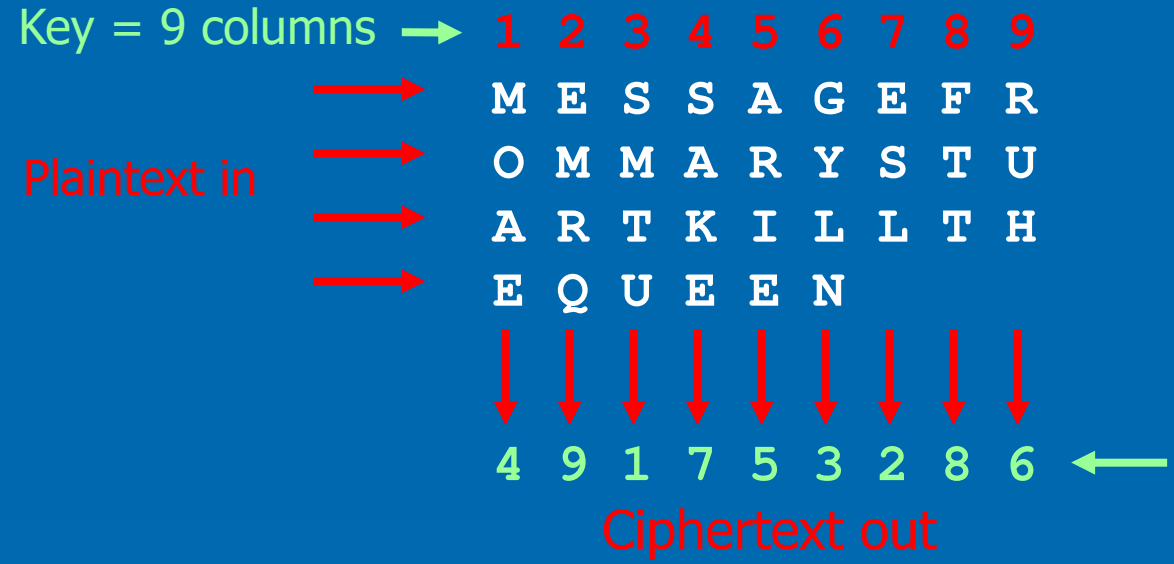
Any questions so far?

Other Ciphers

- So far we considered substitution ciphers
  - Replace one letter (block) with another
- What other basic mechanism can we use to encrypt text?
  - Transposition cipher
    - → Reorder letters (Permutation)

Transposition Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN



Extended key:
order of columns
9! = 362‘880 keys

- Instead of substituting letters, transposition ciphers reorder them
- Write down plaintext on a piece of paper in horizontal rows of *c* characters each
- The ciphertext is read out vertically, column after column

MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Very Old Example of a Transposition Cipher

- Use by ancient Greeks and Spartans, during military campaigns
  - http://en.wikipedia.org/wiki/Scytale
  - Scytale (pronounced like *Italy*, with an S in front)

Transposition Cipher

- If you see a block of ciphertext, how can you guess that it has been encrypted with a Transposition Cipher?
- What about the statistics, i.e. letter frequencies?
  - Ciphertext will have the same relative frequency distribution as normal English text

- How to break a Transposition Cipher?
  - 'Anagramming'
  - Anagram:
    - the result of rearranging the letters of a word or words to produce other words using all the original letters exactly once
  - Examples:
    - Elvis = lives
    - A Homer Simpson = Mr Homo Sapiens
    - Dormitory = Dirty room

Transposition and Substitution

- Transposition Ciphers and Substitution Ciphers as described in the previous slides are not used as stand-alone ciphers in modern systems.
- However, the principles of Transposition and Substitution form the basis of modern ciphers.

- Components of modern ciphers
  - S-Box (Substitution Box)
  - P-Box (Permutation Box) (transposition)

Any questions so far?

Perfect Security

- We consider a cipher to be **strong** if the best attack against it is brute force.
- Then, its security depends on the key length, the resources of the attacker and how long the information needs to be kept secret.
  - "**computational security**"
- But, is there such as thing as *Perfect Security*, i.e. a theoretically unbreakable cipher?
  - Assumption: Attacker has unlimited time and computing resources, maybe even quantum computers
- Yes!
- The **One-time Pad** or **Vernam Cipher** is theoretically unbreakable (perfectly secure)
- Shannon provided a proof for this using Information Theory

One-time Pad (OTP)

- How does it work?
  - For a plaintext message of *n* bits choose *n* **random** bits
    - the one-time pad, only to be used **once**
  - Each bit of the message is 'xor'-ed with the corresponding bit of the random bit string → ciphertext
  - Encryption:
    - $C_i = M_i$ xor K_i
  - Decryption?:
    - Let's 'xor' the ciphertext C with the key K…
    - C_i xor $K_i = (M_i$ xor $K_i)$ xor K_i
    - C_i xor $K_i = M_i$ xor $(K_i$ xor $K_i) = M_i$
    - **$M_i = C_i$ xor K_i**

XOR:
1 xor 1 = 0
1 xor 0 = 1
0 xor 0 = 0
0 xor 1 = 1

Properties of XOR:
(Addition Modulo 2)
Commutative:
A xor B = B xor A
Associative
A xor (B xor C) = (A xor B) xor C

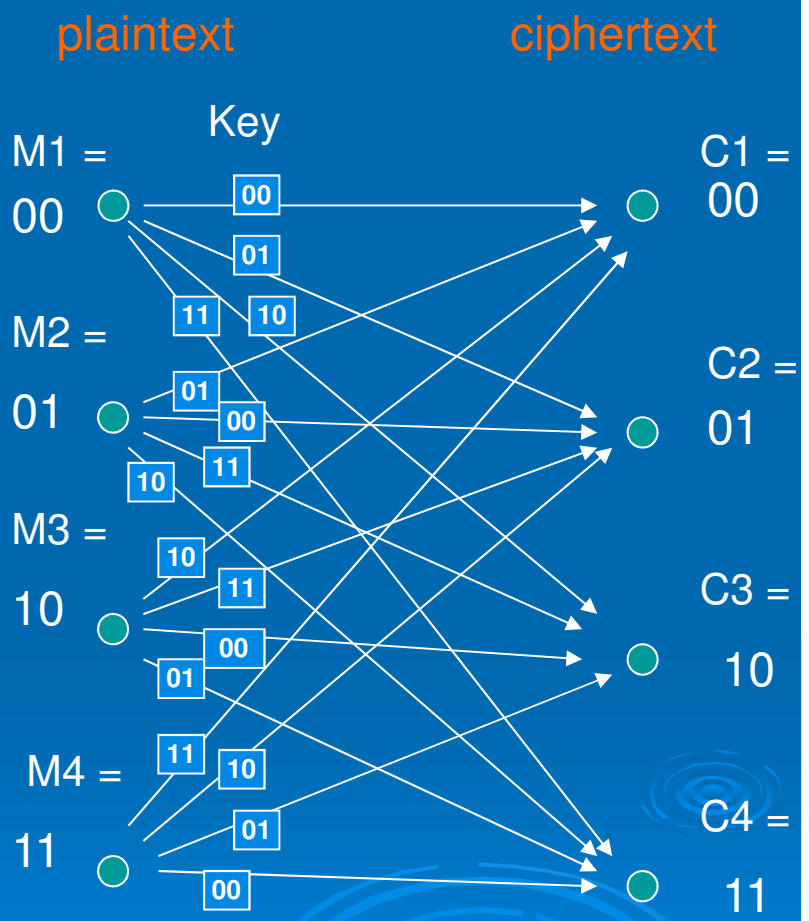
A xor A = 0
A xor 0 = A
A xor B xor A = B

```
Message M:      10010001000100100 10
Pad(key)K:      00110100011101001 00 XOR

Ciphertext C:   10100101011001101 10
```

Why is the One-time Pad unbreakable?

- What would be a condition that guarantees that the cipher is unbreakable?
  - The ciphertext C does not reveal any information about the Messge M (plaintext), in an information theoretic sense
  - This is the case if knowledge of a ciphertext C does not change the probability that a message M was sent
    - P(M|C) = P(M)
    - i.e. M and C are independent random variables, no statistical correlation
  - An attacker has the same chance of guessing the message with or without the knowing the ciphertext
  - Shannon proofs that if P(M|C)=P(M), an attacker gains 0 bits of information from observing the ciphertext.



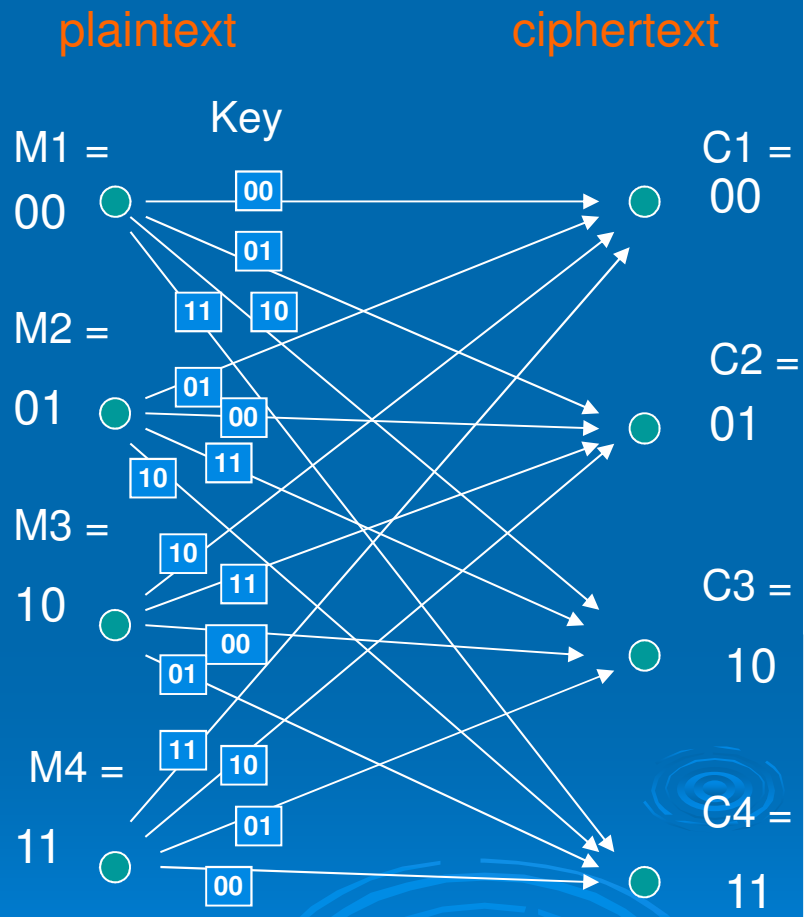
Why is the One-time Pad unbreakable?

- We need to show that: P(M|C) = P(M)

- **Proof idea:**
- P(C1) = ?
- = P(M1)*P(K=00) + P(M2)*P(K=01) + P(M3)*P(K=10) + P(M4)*P(K=11)
- = P(K)*(P(M1) + P(M2) + P(M3) + P(M4))
- = P(K) = ¼ (all keys are equally probable)
- P(Ci) = ¼, for i=1,2,3,4 (independent of M)

- P(Mi | Cj) = ?
- = P(Mi) * P(Cj| Mi)/P(Cj) (Bayes' Theorem)
- = (PMi) * P(K) * 4
- = P(Mi)

- Perfect Security:
  - Probabilty of guessing plaintext is the same with or without seeing the ciphertext.
  - Ciphertext gives absolutely no information about plaintext.



What about Brute Force Attack?

- Brute force attack, how does it work?
  - Try every possible key and see which decryption of ciphertext results in intelligible English text
  - For ‘normal’ ciphers, there is typically only one such key
    - (see tutorial for more detail)
- For one-time pad
  - Given a ciphertext of n bits C, by choosing all possible n-bit keys k, we can generate all possible n-bit plaintexts, which also includes all intelligible English texts.
  - It’s impossible to tell which one is the ‘real’ one
- Brute force attack does not work against OTP

One-time Pad

- If it's perfectly secure and fast, why use any other ciphers?
- What's the catch?
- The key needs to be completely random
  - For a key of n bit length, the Entropy needs to be n bits (no redundancy)
  - It is difficult to generate truly random bit strings
- The key needs to be the same length as the message.
  - And cannot be reused!
- If we want to encrypt a 1 GB file, we need a 1 GB random key
  - → Key distribution problem, not practical
- Compare this with an AES 256-bit key that can be used to encrypt an 'unlimited' amount of data
- In 1945 the U.S. discovered that Canberra-Moscow messages were being encrypted using a one-time pad. However the one-time pad used was the same one used by Moscow for Washington DC-Moscow messages. Combined with the fact that some of the Canberra-Moscow messages included known British government documents, this allowed some of the encrypted messages to be broken.
  - More on this in the Tutorial

Any questions so far?

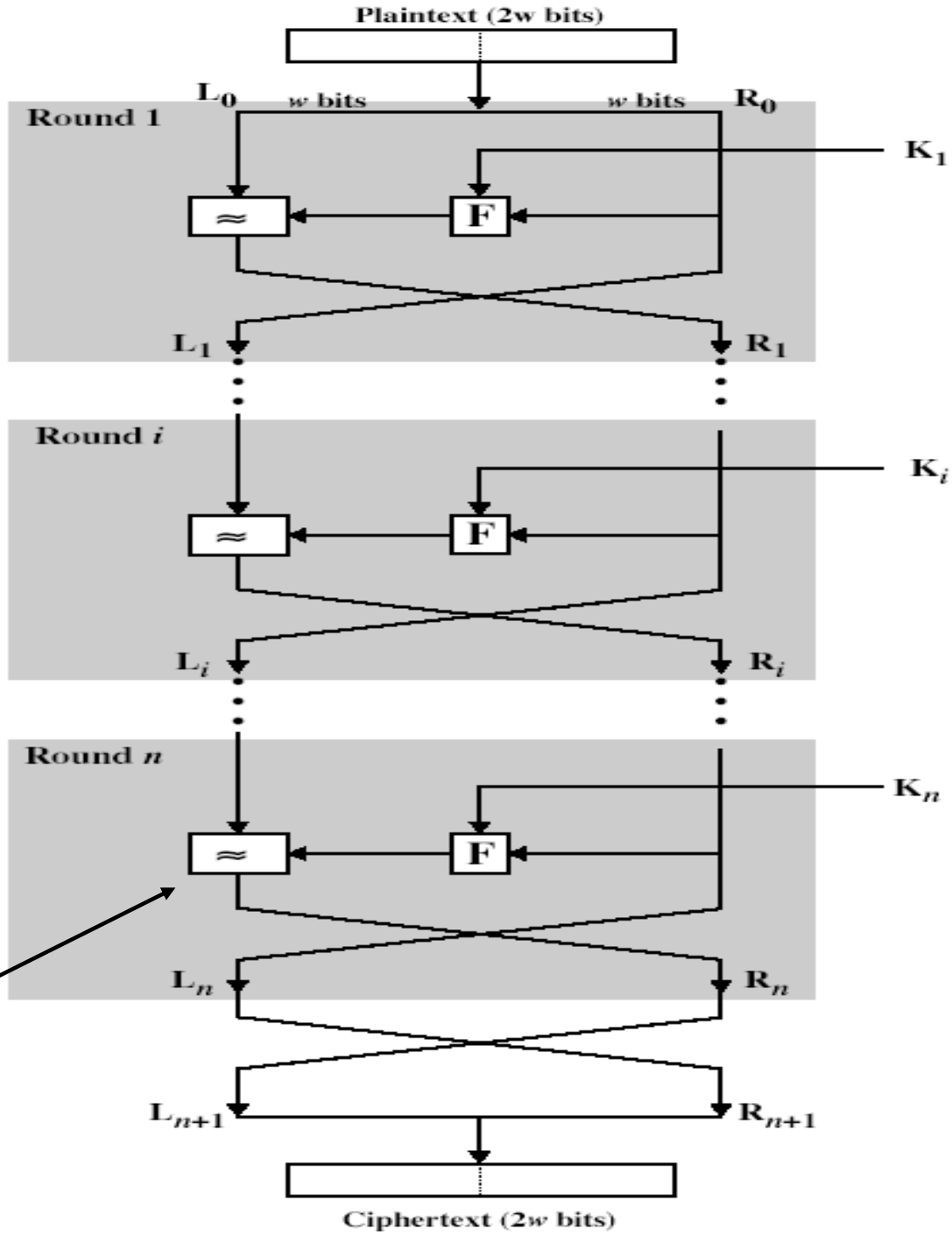
Symmetric Cryptography

Modern Symmetric Ciphers (Secret Key Ciphers)

Modern Ciphers

- Modern Ciphers are often Product Ciphers.
- A product cipher is a composition of functions (ciphers) where each function may be a substitution or transposition
- Iterate several operations to increase security
- 'Feistel' Ciphers are a common class of product ciphers with a specific structure
  - Horst Feistel, Cryptographer working for IBM in 1970s
  - Multiple 'Rounds' of same operation (transposition and substitution)
  - A lot of modern Ciphers are Feistel-Ciphers

Feistel Cipher



XOR

K_i: round Key

Feistel Cipher

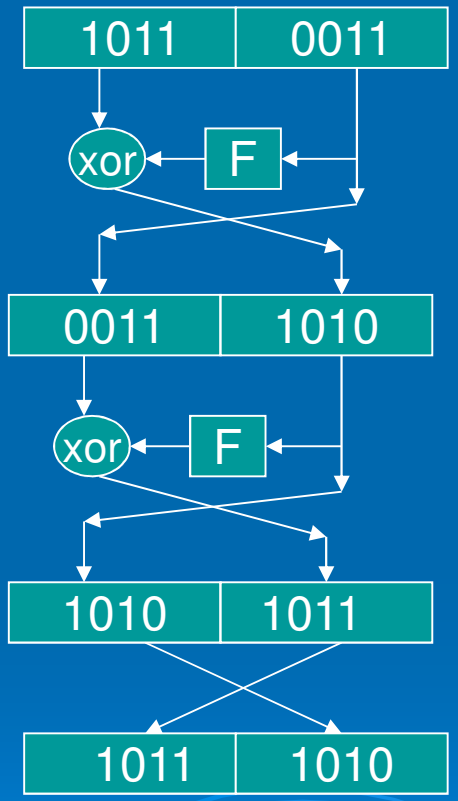
- Combines substitution and transposition
  - Transposition:
    - Swapping of halves
  - Substitution:
    - Replacing left half with something else (Round function F)
      - Called S-box
    - Choice of F determines security of cipher
      - e.g. F should be highly non-linear
- Decryption is same as encryption, but with reverse order of round keys
- Reversibility comes from structure. Function F does not have to be reversible!
  - More on this in Tutorial

Feistel Cipher - Example

- Block size: 8 bits
- 2 Rounds
- Round keys k_i = 1001 = const
- F(k,Ri) = k AND Ri

- Plaintext: 1011 0011

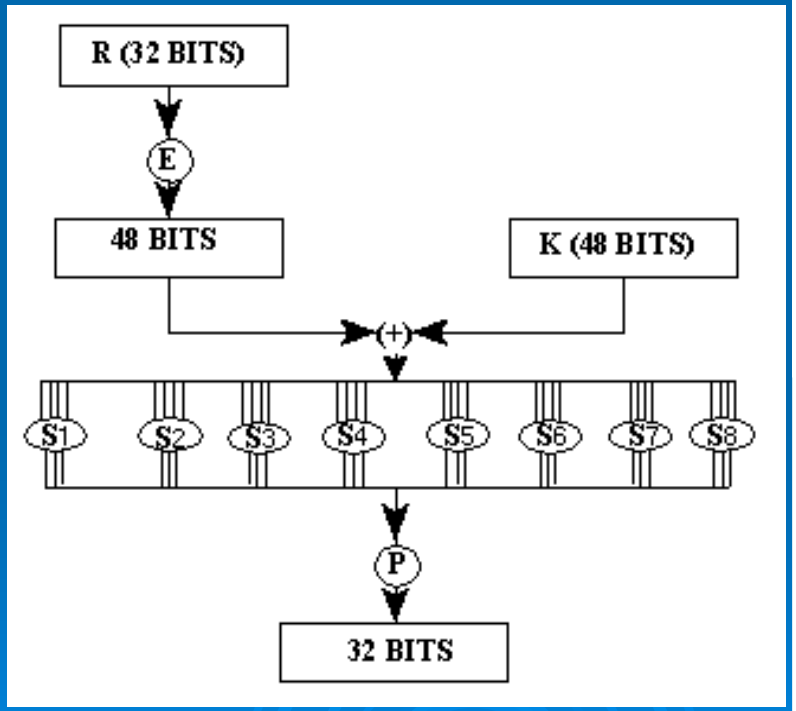
- Ciphertext: 1011 1010



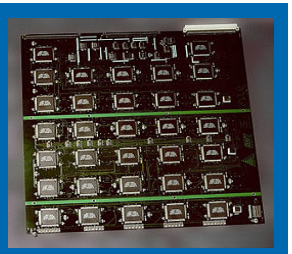
Data Encryption Standard (DES)

- Most widely used cipher for a long time
- Based on IBM's (Horst Feistel's) Lucifer cipher
- NSA made some changes → DES
  - Key length, "S-boxes"
- Standard since 1977
  - National Institute of Standards and Technology (NIST)
- DES is a Feistel Cipher
  - 16 rounds
  - 64-bit blocks
  - 56-bit key (64-bit key less parity)
- Round function F(R,K):
  - Expand 32 to 48 bits
  - S-Box: 6-bit input → 4 bit output
  - Implemented via lookup tables
- No major weakness (break) has been found
  - Brute-force attack is best option
  - Problem: 56-bit key is too short

Function F
DES S-Box



DES Challenges



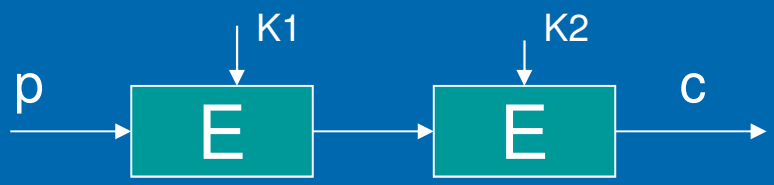
- Series of DES brute force challenges organised by RSA Security
- Goal: Demonstrate inadequacy of 56-bit key length

1997: Internet search distributed.net	Time: 3 months
1998: Purpose built machine (Deep Crack)	Time: 3 days
• Cost: $250K	
• ~ 1800 Custom ASIC chips	
1999: combined effort, distributed.net and Deep Crack	Time: 22 hours
2006: COPACOBANA (120 FPGAs)	Time: 7 days
• Cost: $10K	

- http://en.wikipedia.org/wiki/DES_Challenges
- ➔ 56 bit keys are not secure!
- Corresponding time to crack 128-bit key using COPACOBANA, estimate?
  - Each key bit added doubles required brute-force time
  - 2^{72} * 7 days ≈ 3.3 * 10^{22} days = 9 * 10^{19} years = 90 Billion Billion years

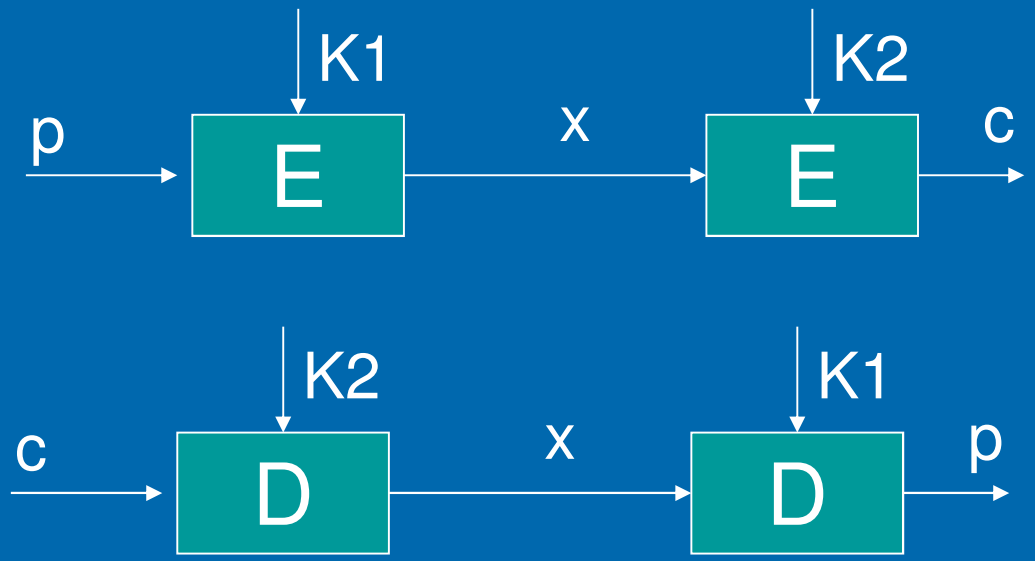
Extending the lifetime of DES

- Q: Given that DES is secure and the only problem is its short key length, how can its lifetime be extended?
- A: Use DES multiple times with different keys
- For example: 2-DES ('Double DES')
  - $c = E_{K2} (E_{K1}(p))$
  - $p = D_{K1} (D_{K2}(c))$



- Is the effective key length=2*56 bits =112 bit?
  - 2-DES is vulnerable to the so-called "meet-in-the middle" attack, which makes it not much more secure than single DES.

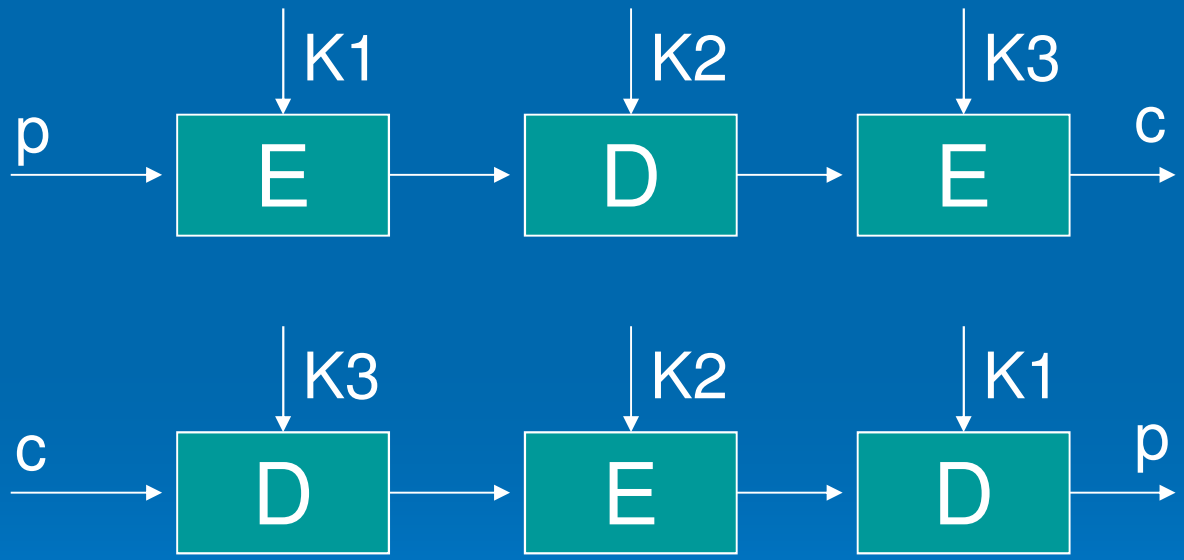
Meet-in-the-middle Attack



- $x = E_{K1}(p) = D_{K2}(c)$
- For a given plaintext-ciphertext pair (p,c)
  - Calculate $E_{K1}(p)$ for all 2^{56} values of K1 (and store them in a table)
  - Calculate $D_{K2}(c)$ for all 2^{56} values of K2
  - If $E_{K1}(p) = D_{K2}(c)$ we have a match and we are likely to have found K1 and K2 for a computational cost of only 2^{57} instead of 2^{112}
  - Trades-off computation with storage cost
    - 'Time-space trade-off'
- What type of attack is this?
  - Known Plaintext attack

3-DES (Triple DES)

- 3-DES-EEE: $C = E_{k1}(E_{k2}(E_{k1}(P)))$
- 3-DES-EDE: $C = E_{k1}(D_{k2}(E_{k1}(P)))$



- But why EDE?
- If K1=K2=K3, then Single-DES compatible

Any questions so far?

Designing a Cipher

- As much an Art as a Science
  - There is no guaranteed recipe for designing a secure cipher, some trial and error is involved
- Goal
  - Computational Security
  - Best attack option should be “brute-force”
    - No shortcuts
    - Key length determines level of security
- Problem
  - It is not possible to proof that a cipher is secure against all possible types of attacks
- What can be done
  - Show that cipher is secure against all **currently known** attacks
  - If, after intense scrutiny of the world’s best cryptographers, no weakness is found, we can have some level of confidence that the cipher is secure.
  - But this is no guarantee. Tomorrow, someone might come up with a new kind of attack …

Advanced Encryption Standard (AES)

- DES was supposed to be replaced in 1989 and 1994, but was re-certified both times
- 1998 NIST announced AES development
  - NIST (US National Institute of Standards and Technology)
- 2000 NIST chooses new cipher as AES

- http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

AES ***Public*** Selection Process

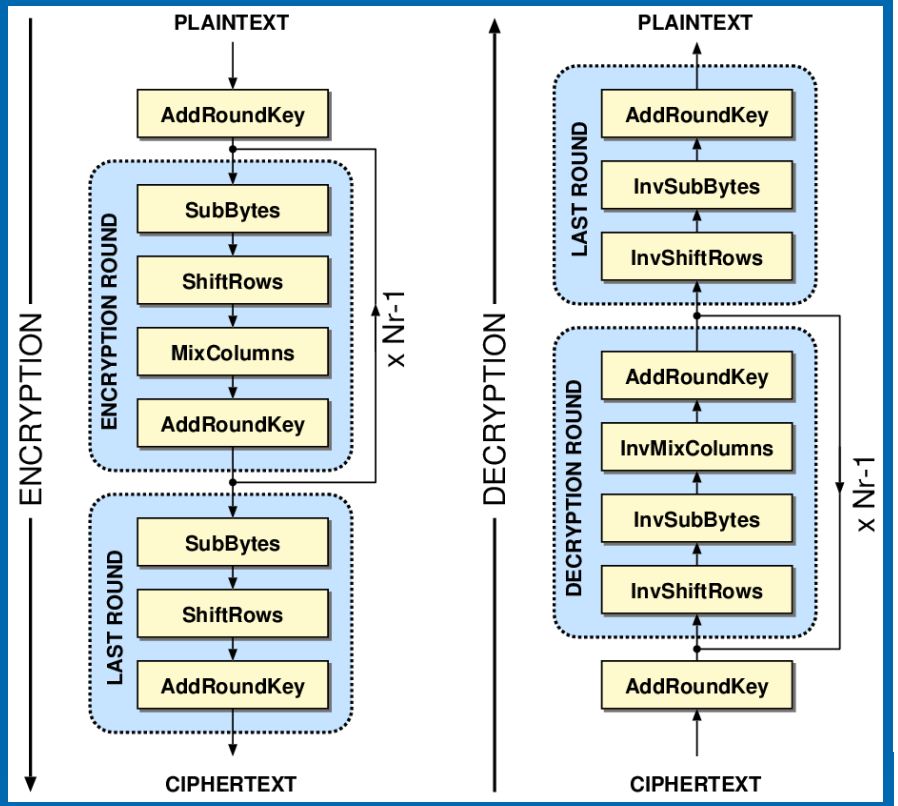
- Selection criteria:
  - Security, cost, flexibility, patent-free, efficiency on wide range of platforms (including 8-bit CPUs)
- 15 candidates
  - 5 broken
  - 5 not as good as others
  - 5 finalists
    - Serpent (Ross Anderson, Eli Biham, Lars Knudsen)
    - Rijndael (Joan Daemen, Vincent Rijmen)
    - Twofish (Counterpane)
      - Feistel structure
    - Mars (IBM)
      - Feistel structure
    - RC6™ (RSA Data Security Inc.)
      - Feistel structure

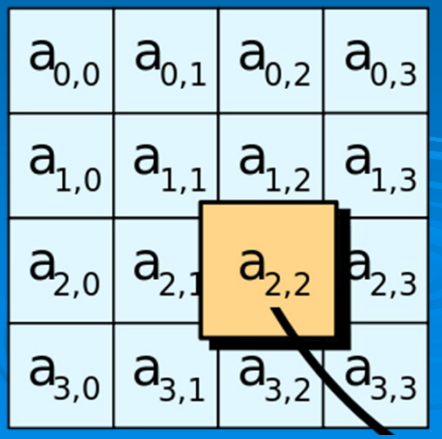
And the winner was …

- Rijndael
  - symmetric block cipher
  - Not a Feistel Cipher!
  - data blocks of 128 bits
  - cipher keys with lengths of 128, 192, and 256 bits
    - “AES-128”, “AES-192”, and “AES-256”
  - designed to handle additional block sizes and key lengths, however they are not adopted in the standard.

AES – How it works in a Nutshell

- Substitution-Permutation (Transposition) Network
- Number of Rounds
  - 128-bit key: 10 rounds
    - fastest
  - 192-bit key: 12 rounds
  - 256-bit key: 14 rounds
    - slowest
- Operations are on a matrix of 4x4 bytes (=128 bits), called the '*state*'





AES – High Level Steps

- Initial Round
  - AddRoundKey
    - Every byte of ‘state’ combined with round key, using bit-wise XOR
      - Round key is derived from Key according to ‘Key Schedule’ (Not covered here)
- Normal Rounds
  - SubBytes—a non-linear substitution step
    - Each byte of the state is replace with another, based on a lookup table
  - ShiftRows—a transposition step
    - Each row of the state is shifted cyclically a certain number of steps
  - MixColumns—a linear transformation on columns
  - AddRoundKey—combine with the round key
    - Same as in initial round
- Final Round
  - Same as normal round, but no MixColumns step

AES Operation

- Choice of transformations such as S-box and permutations in AES are carefully chosen based on mathematical properties of computation in ‘Finite Fields’ or ‘Galois Fields’
  - We won’t cover the details in this course
- A good description of AES
  - http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- Visualisation
  - http://www.youtube.com/watch?v=mIzxpkdXP58

AES Security

- In 2003, US Government states that AES can be used to protect classified information
  - AES-128 for up to SECRET classification
  - AES-192 or AES-256 for TOP SECRET
- So far, no practical attack against AES has been found
  - AES is considered secure
  - … so far

Side Channel Attacks

- Attack on the implementation of a cipher, and not the algorithm itself
- Uses information gained from the physical implementation of a cryptosystem, such as timing information, power consumption, etc., to break a system.

- AES implementations have been broken using Side Channel Attacks
  - Based on timing information for cache access for lookup tables
  - For example
    - Gullasch, David, Endre Bangerter, and Stephan Krenn. "Cache games--bringing access-based cache attacks on AES to practice." *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 2011.
    - http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper031.pdf

- Side channel attacks have been successfully demonstrated for a range of cryptographic systems
- → Never implement crypto algorithms yourself, unless you are an expert!!

AES Performance

- Newer generations of CPUs have specific AES instructions (Intel and AMD)
- Intel i3/i5/i7 with AES-NI instruction set