

Data Security

- Objective: protect data from unauthorized access by intruder
 - Additional line of defense in case of failure of protection/security mechanisms
 - Protection of unsecure channels
- Definitions:
 - *Plaintext*: original message
 - *Ciphertext*: message in encrypted form
 - *Encryption, Decryption*: conversion of plaintext to ciphertext and vice versa
 - *Cryptosystem*: system for encryption and decryption of information. It can be:
 - *Simmetric*: same key used for encryption and decryption
 - *Asymmetric*: different keys
 - *Cryptography, Criptoanalysis*: the study of systems to keep confidentiality, of breaking cryptosystems respectively

Potential threats

- There are different types of threat to a cryptographic system depending on the amount of additional info available to the intruder
 - *Ciphertext-only attack*: self explanatory;
 - *Known-plaintext*: a considerable amount of corresponding plain text is available;
 - *Chosen-plaintext*: the intruder can obtain ciphertext corresponding plain-text of his choice
- A robust cryptosystem should be able to stand the most severe threats

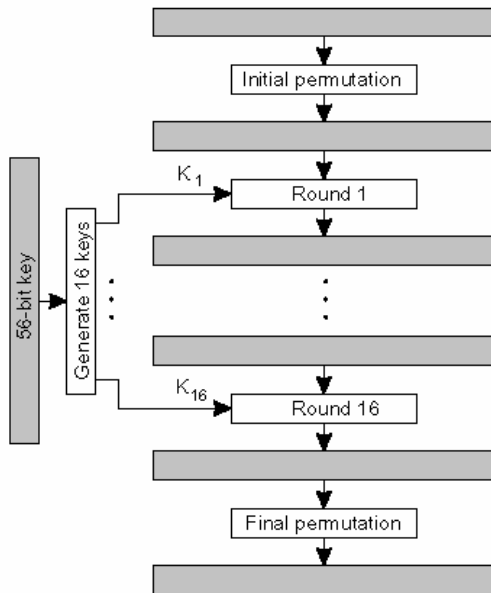
Conventional Cryptography

- Based on substitution ciphers which are not very robust. Examples
 - *Caesar cypher*: replace each letter with the third one following it according to the alphabetic order
 - “Julius loves Cleopatra” → “mxolxv oryhv fohrsdwud”
 - Can be generalized changing the amount of shift, but it is still trivial, and the number of keys is limited to 25
 - *Simple substitution*: any permutation of letters can be mapped to English letters
 - Each permutation is a key, so there are $26!$ ($> 10^{26}$) keys
 - Can be easily broken using statistical analysis
 - *Polyalphabetic ciphers*: use n substitution alphabet ciphers in sequence
 - More robust than the previous; can be broken if period n is discovered
 - unbreakable variant (called *one-time pad*): n is equal to message size

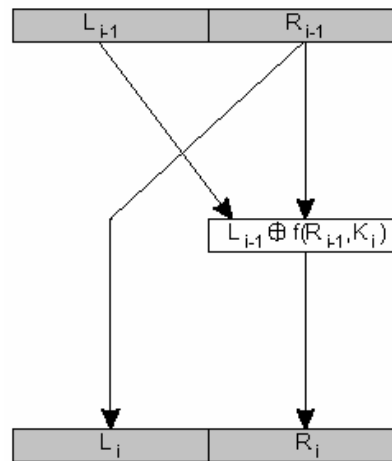
Modern Cryptography

- Modern cryptosystems are can be divided in:
 - Private key systems: $P=D_k(E_k(P))$ (symmetric)
 - Public key systems: $P=D_{k1}(E_{k2}(P))$ (asymmetric)
- These system have the following features:
 - They are specialized for binary data,
 - They are based on a open design,
 - They rely on algorithms for which an exhaustive search is impractical because computationally too intensive

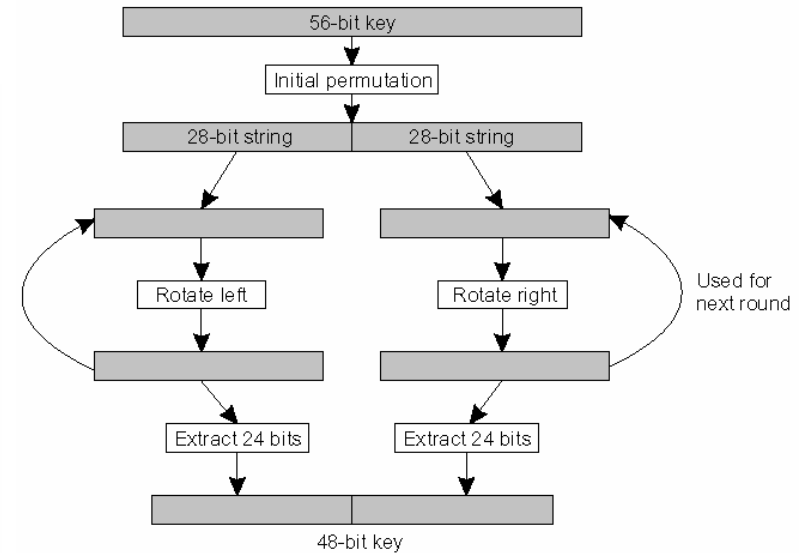
DES: Data Encryption Standard



Basic DES scheme



Outline of one encryption round



Key generation for each round

- DES is a private key cryptography standard
 - It is the official encryption standard for the US federal government but it is no longer considered safe and is being replaced by a 128 bit key variant
- The crucial aspect is that the key must be sufficiently long
 - Current length (56 bit) has been broken using brute force attack

Private Key

- Pro:
 - Relatively fast
 - Widespread use thanks to standardization
 - Public domain (i.e. not patented)
- Con:
 - Requires key to be known to both parties (*key distribution problem*)
 - Cannot be used for other applications such as digital signatures, etc.

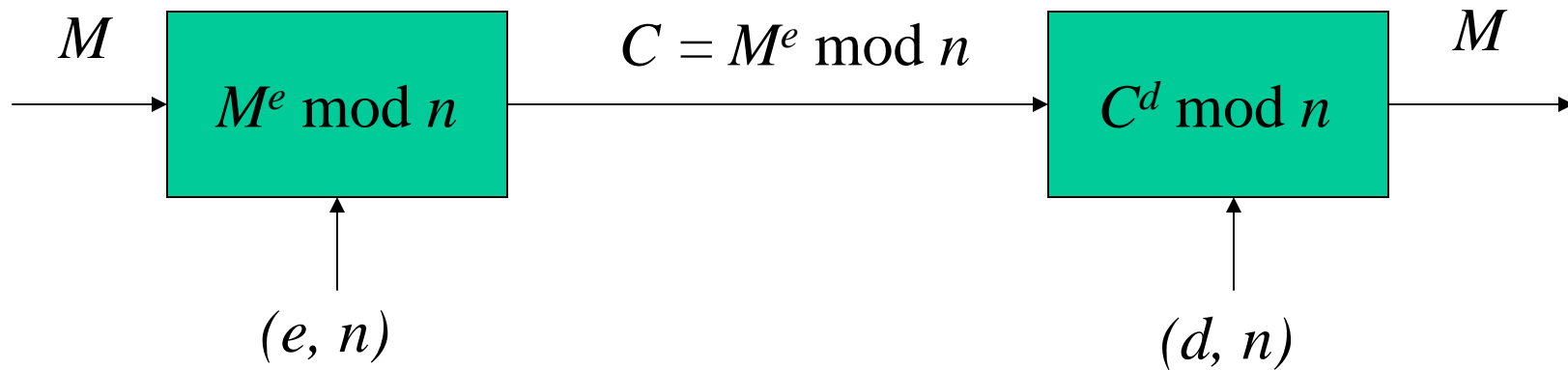
Public Key: principles

- Basic scheme suggested by Diffie and Hellman is based on *one-way* functions
 - one-way function:
 - given x , computing $f(x)$ is easy
 - given y , finding x such that $y=f(x)$ is very hard
 - therefore f^{-1} is hard to derive even if f is known
- *trapdoor one-way* function: a one-way function for which f^{-1} is easy to compute, provided a certain additional piece of information is provided

Rivest-Shamir-Adleman (RSA) method

- Plaintext is divided in blocks, each represented as a number between 0 and $n - 1$
 - encryption: $C = M^e$ modulo n
 - decryption: $M = C^d$ modulo n
- The two keys e and d are determined as follows:
 - choose two large prime numbers p and q ,
 - compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$,
 - choose a large integer d so that is prime relative to z , i.e. $\text{GCD}(d, z) = 1$
 - compute e so that $e \times d = 1 \pmod{z}$

RSA scheme



Case study: Digital signature

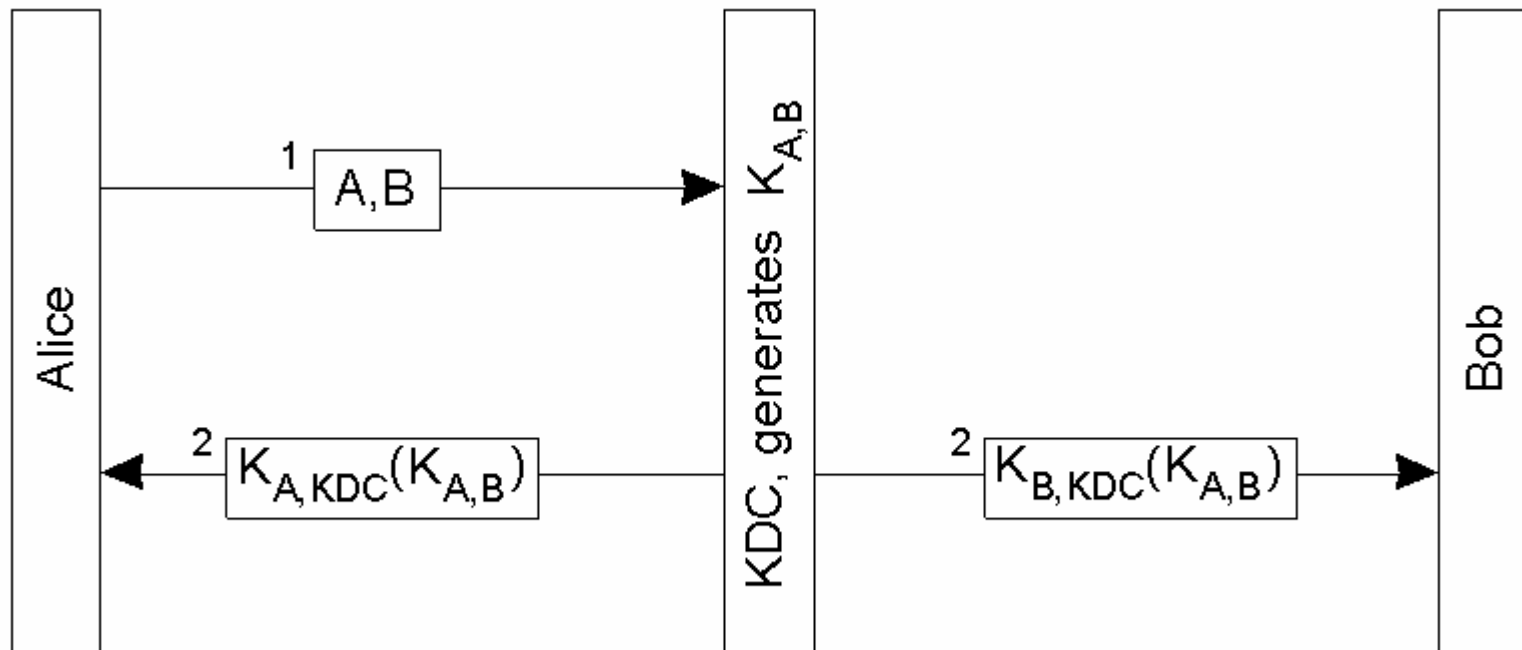
- The purpose of a digital signature system is to ensure the authenticity of a document
- Note that a public key cryptographic system naturally doubles as a digital signature system
 - encryption with the private key is equivalent to *signing* a message
 - decryption with the public key is equivalent to *verifying* the message

Case study: Kerberos

- Kerberos is a system for authentication on distributed systems
 - Started as part of the Athena Project at MIT
 - Third-party authentication scheme
- Based on private key encryption and uses DES
 - Kerberos maintains a database of users and their private keys
 - The private key on the client is obtained from the user's password with a one-way function
 - $K_U = f(\text{password})$

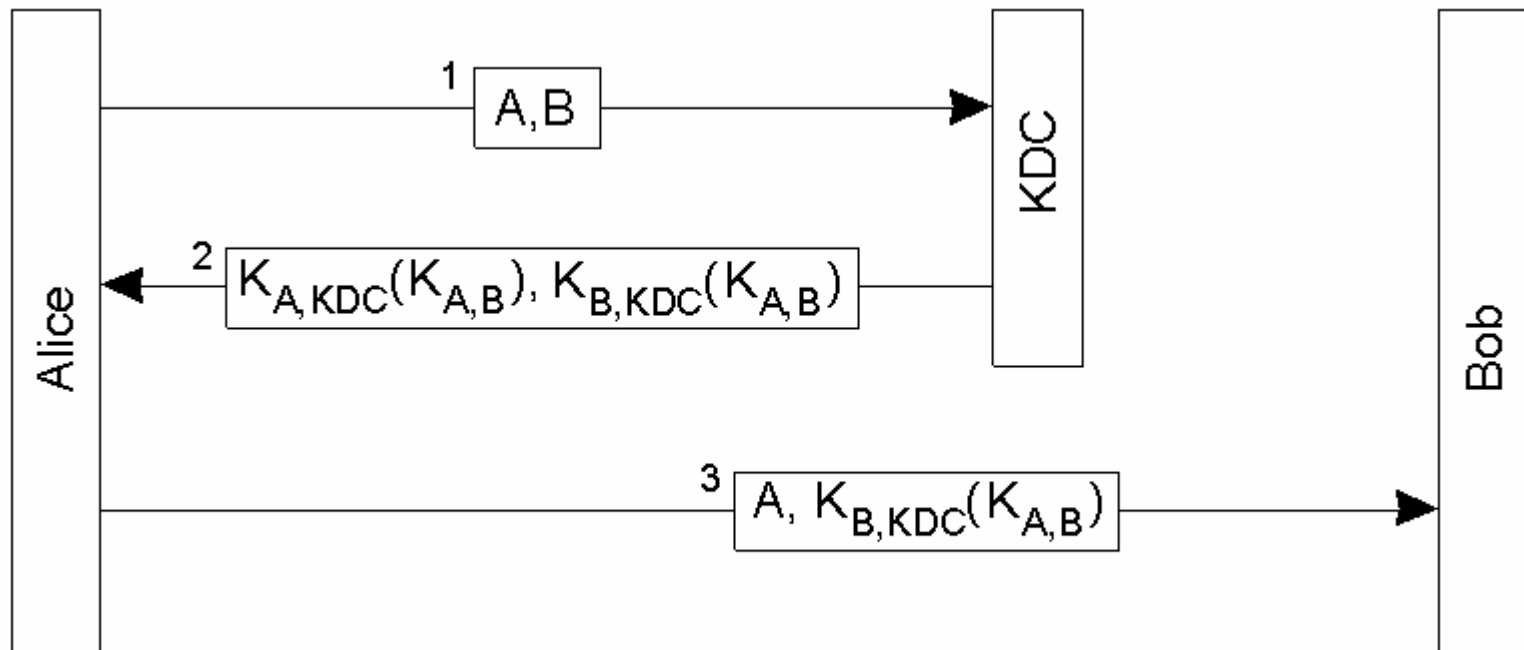
Authentication Using a Key Distribution Center (1)

- Alice asks the KDC for a session key to set up a connection to Bob



Authentication Using a Key Distribution Center (2)

- Using a ticket and letting Alice set up a connection to Bob.



Kerberos scheme

