L91D - IP Security Introduction

Introduction to IP Security Components

What is Security?

- **Seen in the context**
  - of computer scientist and network managers
- **Security is the**
  - science (though some would call it an art) of protecting computers, network resources and information against unauthorized access, modification and/or destruction
- **Generally four topics are involved**
  - Confidentiality
  - Authentication
  - Integrity checking
  - Non-repudiation

 IP Security Intro, v4.5 2

Security in the context of the Internet 1

- **Security Architecture for the Internet Protocols**
  - RFC 1825 (obsoleted by 2401/4301) defines four topics:
- **Confidentiality (Secrecy, Privacy)**
  - The property of communicating such that the intended recipients know what was being sent but unintended parties cannot determine what was sent
- **Authentication**
  - The property of knowing that the claimed sender is in fact the actual sender
- **Integrity checking**
  - The property of ensuring that data is transmitted from source to destination without undetected alteration

Security in the context of the Internet 2

- **Non-repudiation**
  - The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data
- **These four topics are implemented by means of**
  - cryptography (today a topic of mathematic)
  - number theory
  - hash functions (one way functions)
  - message digest
  - appropriate security protocol methods and server functions

Cryptology and Steganography

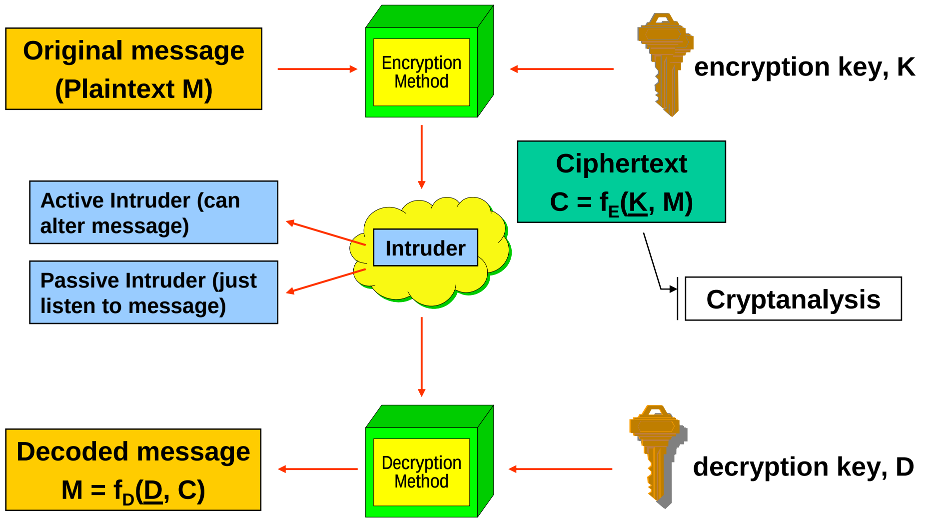
- **Steganography**
  - The art of hiding secret information in other information
- **Cryptology**
  - The art of devising ciphers (cryptography) and breaking them (cryptanalysis)
- **Cryptography**
  - Greek words
    - κρυπτο means hidden or secret
    - γραφη means writing
  - cryptographers invent clever ciphers
- **Cryptanalysis**
  - cryptanalysts attempt to break these ciphers

Basic Cryptography Terms 1

- **Encryption**
  - is the process of disguising a message in such that the original content is hided
  - plaintext (cleartext, readable message) is converted to ciphertext (unreadable, disguised message)
- **Decryption**
  - is the process turning ciphertext back into the original plaintext
- **Purpose of Encryption/Decryption**
  - confidentiality (secrecy, privacy)
  - only authorized entities can decrypt data based on knowledge of cryptographic keys

L91D - IP Security Introduction

Basic Cryptography Terms 2



Basic Cryptography Terms 3

- **Cryptographic systems consists of**
  - Complex mathematical function called <u>algorithm</u> for encryption and decryption
  - One or more secret or public values called <u>keys</u>
    - known only to the parties involved in secure communication (exception: public keys are known to anyone)
  - Note:
    - if encryption is based on secrecy of the algorithm itself, the algorithm must be heavily guarded, once revealed every party involved must change it
    - in modern cryptographic system the algorithms are available to anyone (are standardized), the secrecy of data is ensured by cryptographic keys
    - compare it with mass-produced door lock which protects your house by your individual door key

Basic Cryptography Terms 4

- **A strong algorithm**
  - withstood the attempts of clever guys to break it
  - is resistant to common cryptographic attacks against it
  - breaking the protected data needs trying all possible keys to decrypt -> brute-force attack
  - time needed for brute-force attack is extremely long
- **A good key**
  - is known only to the appropriate person(s), is not easily guessable and is sufficiently long enough to withstand brute-force attacks
- **Two basic concepts about keys**
  - Secret-Key versus Public-Key

 IP Security Intro, v4.5 9

Basic Cryptography Terms 5

- **So the real secrecy depends on the key and not on the algorithm**
- **Key length is a major design issue**
  - trying out all possible keys to find the right key
  - brute-force attack
  - the more possibilities the higher the work factor
    - work factor increases exponentially with key length
      - $2^{(\text{number of bits})}$
      - 2^{16} means 65536 possibilities, 2^{56} means $7*10^{16}$ possibilities
    - increasing the key length by one bit means doubling the range of possible keys
  - time to decrypt message by brute-force attack versus usefulness (lifetime) of message

 IP Security Intro, v4.5 10

Basic Cryptography Terms 6

- **Source of a key is also important**
  - e.g. if key generation of 128-bit secret key depends on a 8 character password then a cryptanalyst must tryout only all combinations of printable 8 character password instead of 2^{128} possibilities
    - feeding it with all possible words of a dictionary will produce interesting results because of the human factor
  - dictionary attack
    - even if brute-force attack would last to long with today's computer resources a valid key can be found soon in such a case

 IP Security Intro, v4.5 11

Basic Cryptography Terms 7

- **Three basic attacks for breaking an encryption schema**
  - ciphertext only attack
    - the cryptanalyst has a quantity of ciphertext but no plaintext
      - brute-force attack and recognition of meaningful text
      - enough ciphertext is necessary for this
    - modern algorithms are just to good to fall to this kind of attack
  - know plaintext attack
    - the cryptanalyst has a quantity of matched ciphertext and plaintext and then recovers the key
    - this might sound useless but if later a message is sent with the same key used to encrypt the attacker can take the broken key and read the message
    - great help against German Enigma

 IP Security Intro, v4.5 12

Basic Cryptography Terms 8

- chosen plaintext attack
  - the attacker has the ability to encrypt pieces of plaintext of his own choosing
  - e.g. that would be possible in public-key systems
  - then he recovers the key based on the encrypted result
- **A good cryptographic system**
  - should be resistance against all three sorts of attacks

 IP Security Intro, v4.5 13

Threats through Intrusion

- **Passive intruder**
  - obtain information about something not intended for him
    - e.g. passwords, credit-card numbers, etc.
  - may misuse this information to break into systems, order things, etc. causing damage
  - aspect is privacy
- **Active Intruder**
  - manipulation of messages on the fly
  - one aspect is integrity checking
  - replay attack
  - even if he cannot read a encrypted message damage, confusion may arise

 IP Security Intro, v4.5 14

Cryptographers Terminology

- **Cryptography is a science**
  - of transforming data in a seemingly bizarre ways to accomplish surprisingly useful things
  - practised by intelligent mathematicians called cryptographers given complicated answers to what would appear to be a simple question
  - Question of person of average intelligence:
    - “If I did this, that and another thing, would that then be secure?
  - Answer of cryptographer:
    - “It is computationally infeasible that your security mechanism could be broken within the relevant lifetime of the data you wish to protect, assuming that computing power continues to improve at or near its current rate of growth”
  - Person of average intelligence: “Huh?

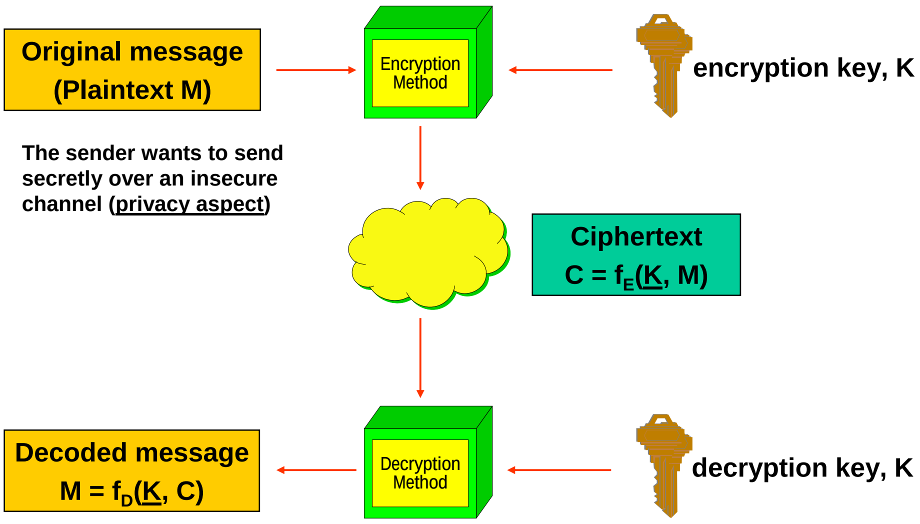
 IP Security Intro, v4.5 15

Secret-Key Algorithms 1

- **Single secret key K used by sender and receiver**
  - Called symmetric algorithms
- **Methodology**
  - $C = f_E(\underline{K}, M)$
  - $M = f_D(\underline{K}, C)$
    - C (Ciphertext)
    - K (Key)
    - M (Plaintext)
    - E (Encryption)
    - D (Decryption)
    - $f_E(\underline{K}, M)$ (encryption function performed on M using K)
    - $f_D(\underline{K}, C)$ (decryption function performed on C using K)

 IP Security Intro, v4.5 16

Secret-Key Algorithms 2



Secret-Key Algorithms 3

- **Characteristics:**
  - Based on simpler mathematical operations than public-key algorithm
    - hardware assist
  - Faster to compute than public-key algorithm
    - wire-speed encryption possible
  - Used for bulk encryption when data privacy is required
    - high volume mechanism
  - Key-length 40 - 256 bit
    - 56 was sufficient in the 80´s (21min to break nowadays by NSA)
    - 128 is sufficient to withstand brute-force attacks based on today's computer technology
    - 168 and above is far away from being necessary (10^{17} years to break with nowadays technology)

Secret-Key Algorithms 4

- **Characteristics (cont.):**
  - Key management can be a problem
    - Secret key must be exchanged between parties via secure channel before any encryption can occur
    - Note: the security of a cryptographic system heavily depends on the security of the key exchange
- **Examples:**
    - DES … Data Encryption Standard (40, 56 bit)
    - TripleDES (112, 168 bit)
    - IDEA … International Data Encryption Algorithm (128 bit)
    - Blowfish
    - RC4/5 … Ron Codes 4/5
    - AES … Advanced Encryption Standard (128, 192, 256 bit)
    - …

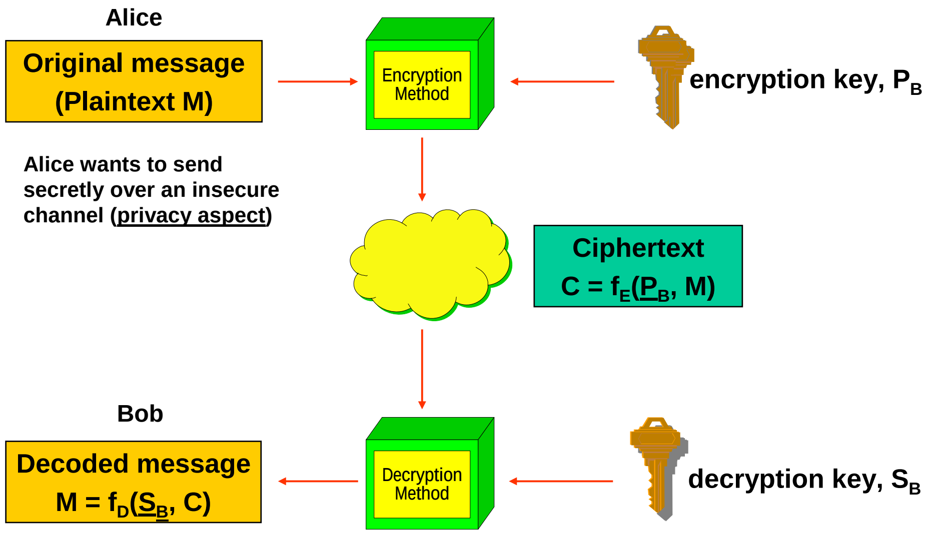
Public-Key Algorithms 1

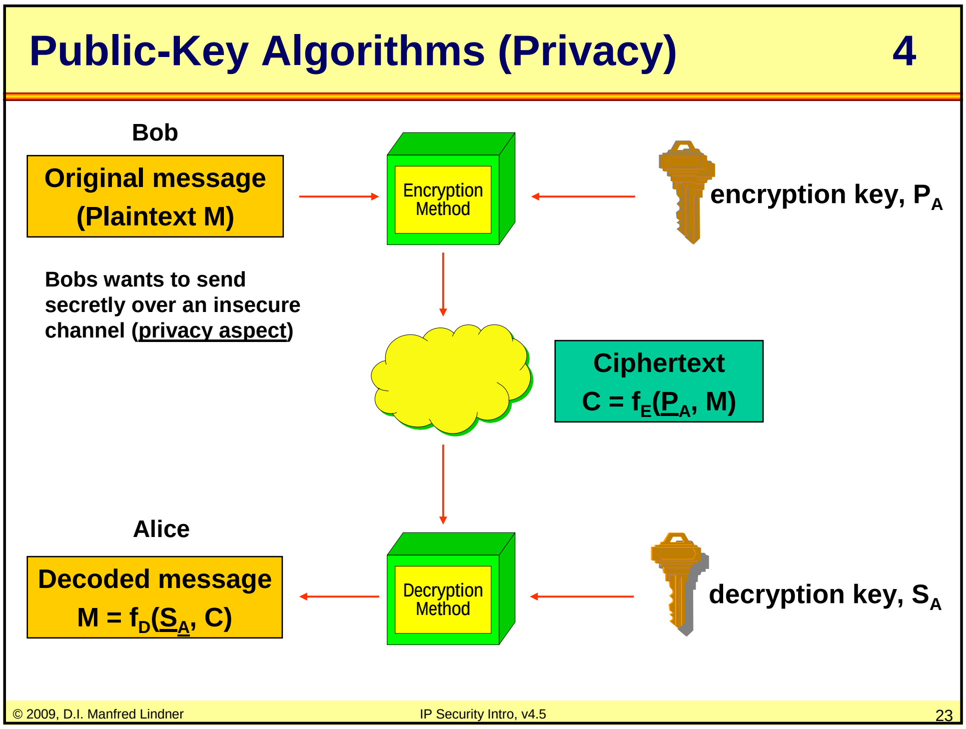
- **Based on unidirectional security association**
  - between two parties wanting to exchange information in a secured way
- **A pair of keys is used**
  - Private Key used by one party
    - key kept secret in one system
    - to sign messages to be sent to the other party for authentication
    - to decrypt messages received from the other party
  - Public Key used by the other party
    - key may widely be published to many systems
    - to encrypt messages to be sent to the other party for privacy
    - to verify messages received from the other party for authentication
- **Called asymmetric algorithms**

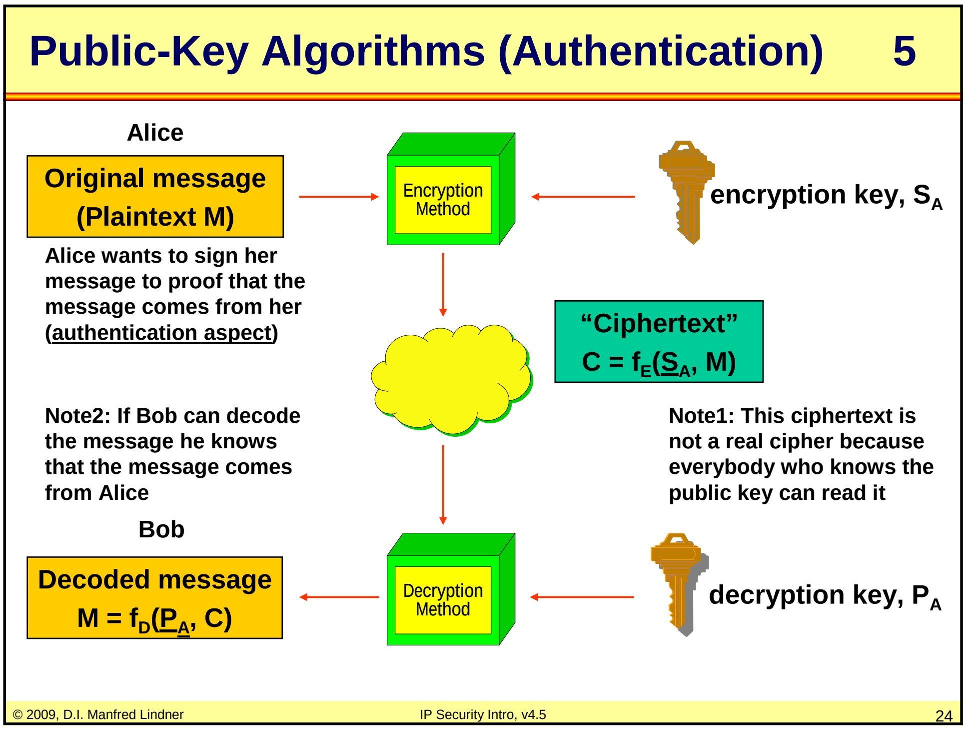
Public-Key Algorithms 2

- **Methodology**
  - S … Private Key, P … Public Key
  - Security association between Alice and Bob
    - Alice generates one key pair (P_A, S_A), keeps S_A secret in her system and give P_A to Bob
  - Security association between Bob and Alice
    - Bob generates one key pair (P_B, S_B), keeps S_B secret in his system and give P_B to Alice
  - Encrypted messages from Alice to Bob
    - $C = f_E (\underline{P_B}, M)$
    - $M = f_D (\underline{S_B}, C)$ done by Bob to decrypt
  - Encrypted messages from Bob to Alice
    - $C = f_E (\underline{P_A}, M)$
    - $M = f_D (\underline{S_A}, C)$ done by Alice to decrypt

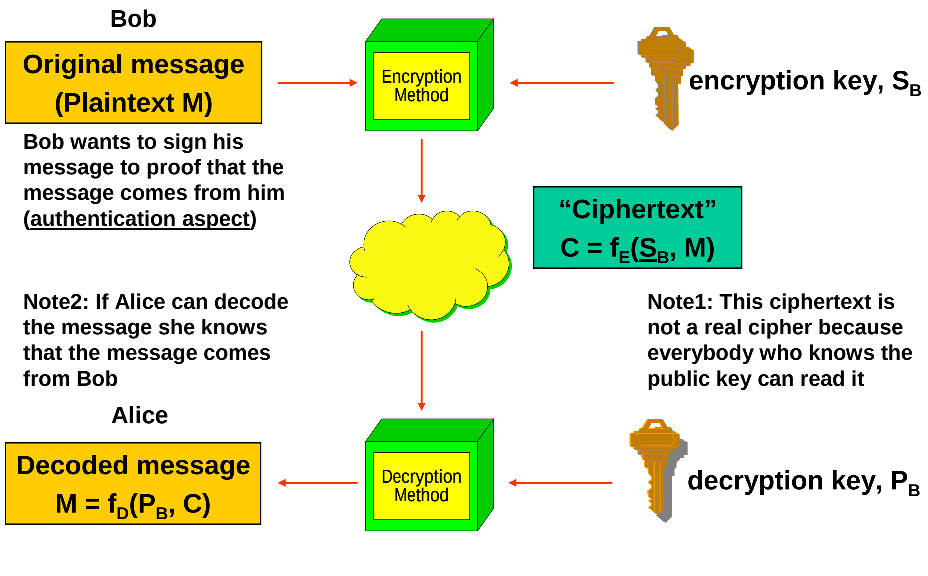
Public-Key Algorithms (Privacy) 3




Public-Key Algorithms (Privacy)
4
Bob
Original message
(Plaintext M)
Encryption Method
encryption key, P_A
Bobs wants to send secretly over an insecure channel (privacy aspect)
Ciphertext
$C = f_E(P_A, M)$
Alice
Decoded message
$M = f_D(S_A, C)$
Decryption Method
decryption key, S_A
© 2009, D.I. Manfred Lindner
IP Security Intro, v4.5
23


Public-Key Algorithms (Authentication)
5
Alice
Original message
(Plaintext M)
Encryption Method
encryption key, S_A
Alice wants to sign her message to proof that the message comes from her (authentication aspect)
"Ciphertext"
$C = f_E(S_A, M)$
Note2: If Bob can decode the message he knows that the message comes from Alice
Note1: This ciphertext is not a real cipher because everybody who knows the public key can read it
Bob
Decoded message
$M = f_D(P_A, C)$
Decryption Method
decryption key, P_A
© 2009, D.I. Manfred Lindner
IP Security Intro, v4.5
24

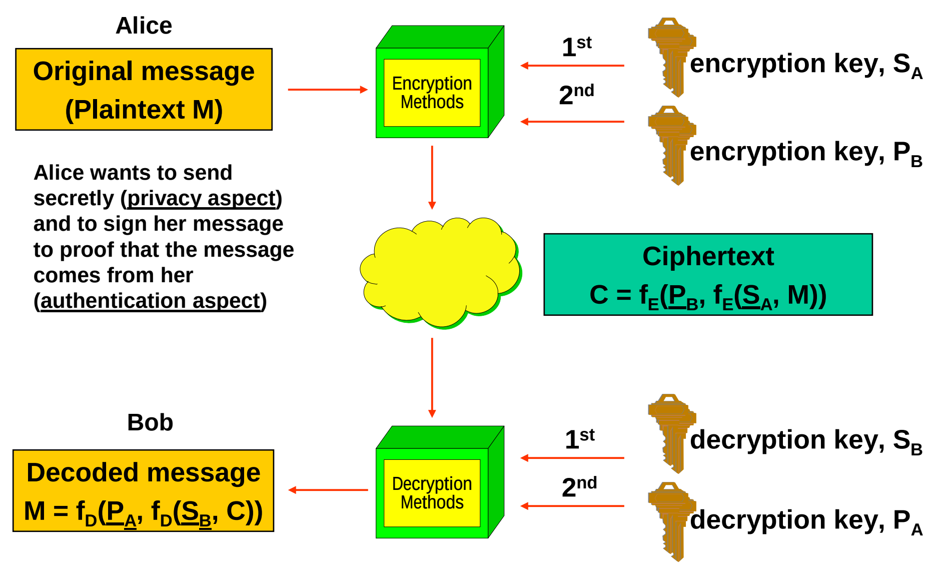
Public-Key Algorithms (Authentication) 6



Public-Key Algorithms 7

- **Algorithm use different keys for encryption and decryption**
- **Because of the mathematical properties of the algorithm**
  - the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key
    - privacy aspect
  - the encryption key cannot (at least in any reasonable amount of time) be calculated from the decryption key
    - authentication and non-repudiation aspects
- **In theory you can combine**
  - privacy and authentication aspects in one schema

Public-Key Algorithms (Both Aspects) 8



 IP Security Intro, v4.5 27

Public-Key Algorithms 9

- **Characteristics:**
  - Based on more complex mathematical operations than secret-key algorithm
  - Slower to compute than secret-key algorithm
    - 1000 times slower in SW, 100 times slower in HW
  - Therefore often used
    - to distribute secret-keys in a secure way in case of privacy aspect should be achieved by secret-key encryption
    - to generate a signature of the message for authentication and integrity checking reasons (low volume mechanism)
  - Key-length 512 - 2048 bit
    - note: you cannot compare this with the length used for secret-keys because the algorithm families differ greatly in their underlying design

 IP Security Intro, v4.5 28

Public-Key Algorithms 10

- **Characteristics (cont.):**
  - Key management tends to be simpler compared to secret-key algorithms
    - one key of the pair can usually be made public
- **Examples:**
  - (Diffie-Hellmann-Merkle)
  - RSA … Rivest, Shamir and Adleman
  - ElGamal … El Gamal
  - Elliptic curve algorithms
  - DSS … Digital Signature Standard