Electronics and Computer Science
University of Southampton

CM214-COMP2008
Data Communications and Networks

Network Security - 2

Karl R. Wilcox
krw@ecs.soton.ac.uk

Objectives

- To look at how the tools and technologies of security are assembled into secure systems

- (Peterson & Davie, Sections 8.1-3)

Review

- We have looked at components that provide:
  - Fast, reasonably secure encryption using secret keys
    - DES, Triple DES, IDEA
  - Slower, very secure encryption using public keys
    - RSA
  - Message digests
    - MD5

Building Security Systems

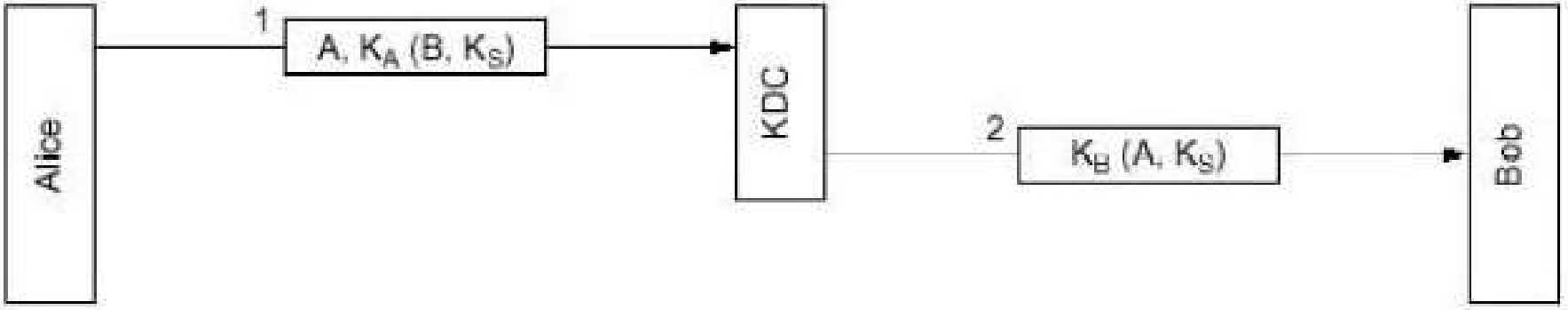
- We can combine components to:
  - Authenticate parties & agree session key
    - Needham-Schröder key distribution protocol
  - Authenticate parties & their privileges via an intermediary
    - Kerberos
  - Send secure e-mail
    - PGP2
  - Securely access online services
    - SSH / SFTP

Terminology

- A, B Identification strings for "Alice" and "Bob"
- K_A, K_B Encryption keys for Alice & Bob
- K_S Encryption keys for this session
- P Plaintext of the message
- R_n A randomly chosen number
- $K_B(A,R_1)$ Alice's identification string and a random number encrypted using Bob's key
- $K_A(K_B(A,R_1))$ Above, further encrypted with Alice's key

Use of an Intermediary

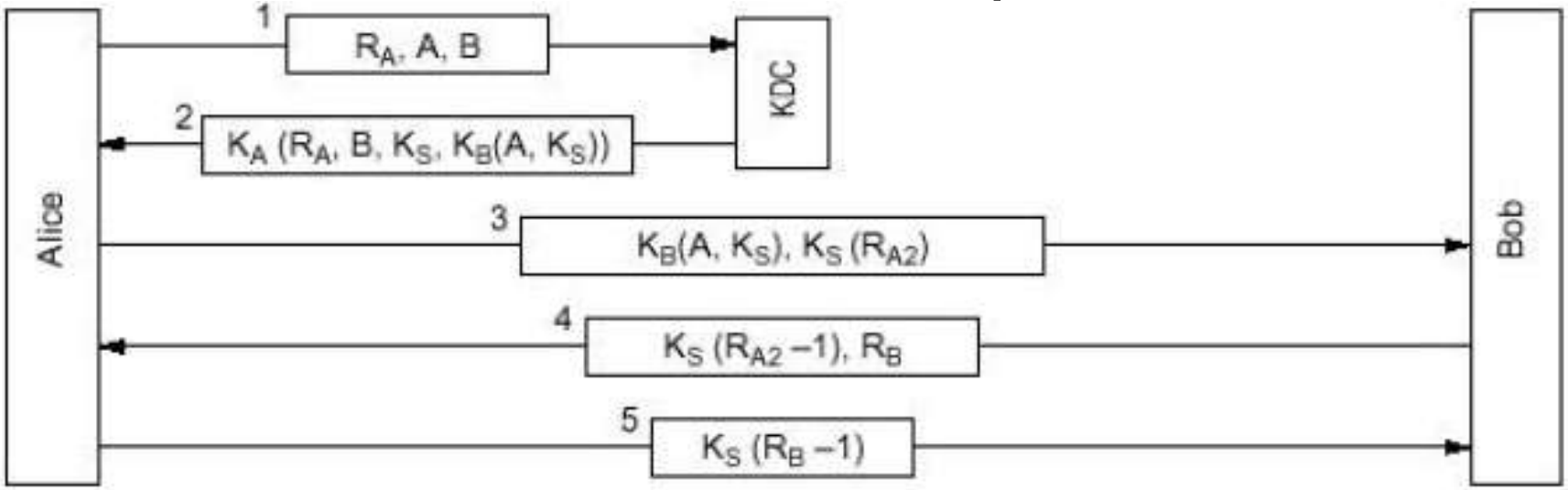
- Simple use of key distribution centre



- Vulnerable to message cloning
- Does not validate B's identity to A

A Better intermediary

- The Needham-Schröder protocol

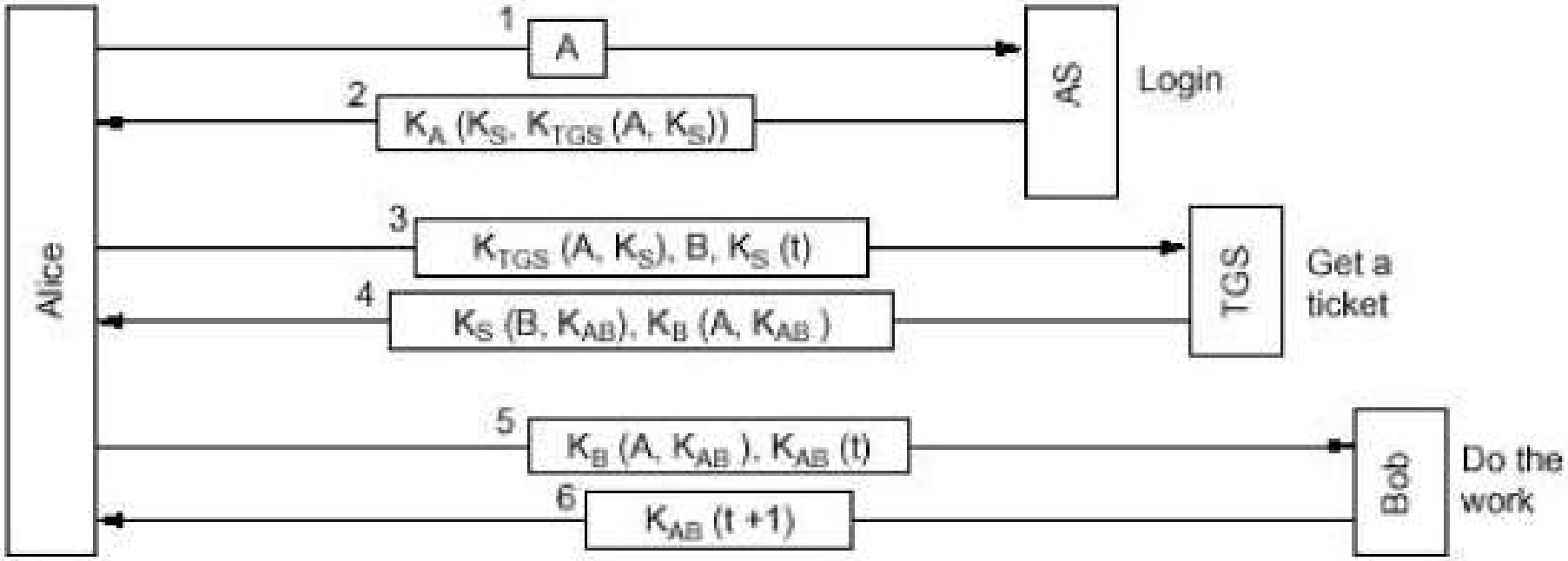


- A & B are sure of each other's identity
- Both know the session key is valid

Kerberos

- A complete system that can:
  - Authenticate users
  - Authenticate systems
  - Provide levels of privilege
    - Including timestamps
    - Validity periods

Kerberos Example

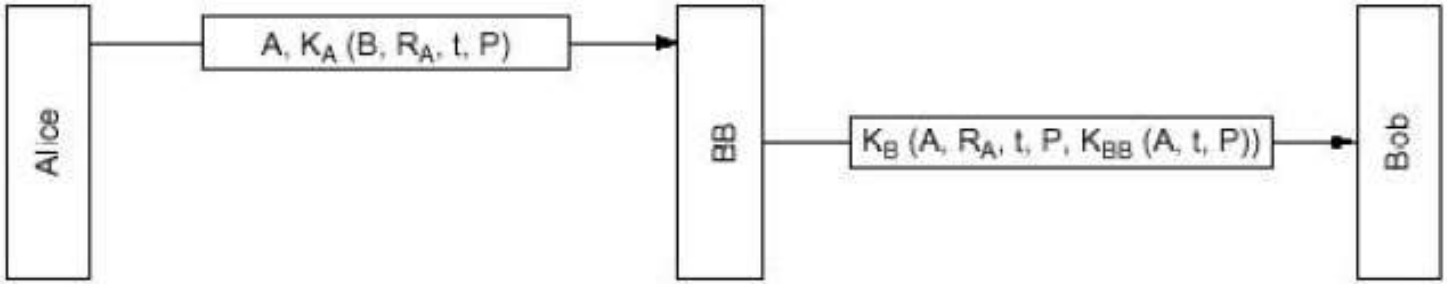


AS = Authentication Server

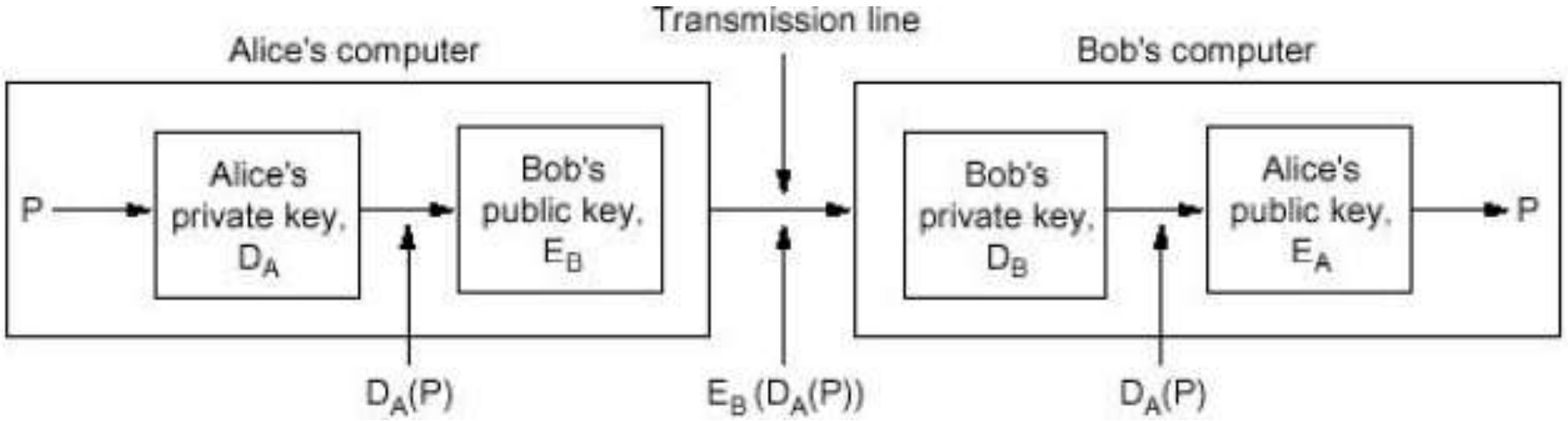
TGS = Ticket Generation Server

Non-repudiation

Using secret keys



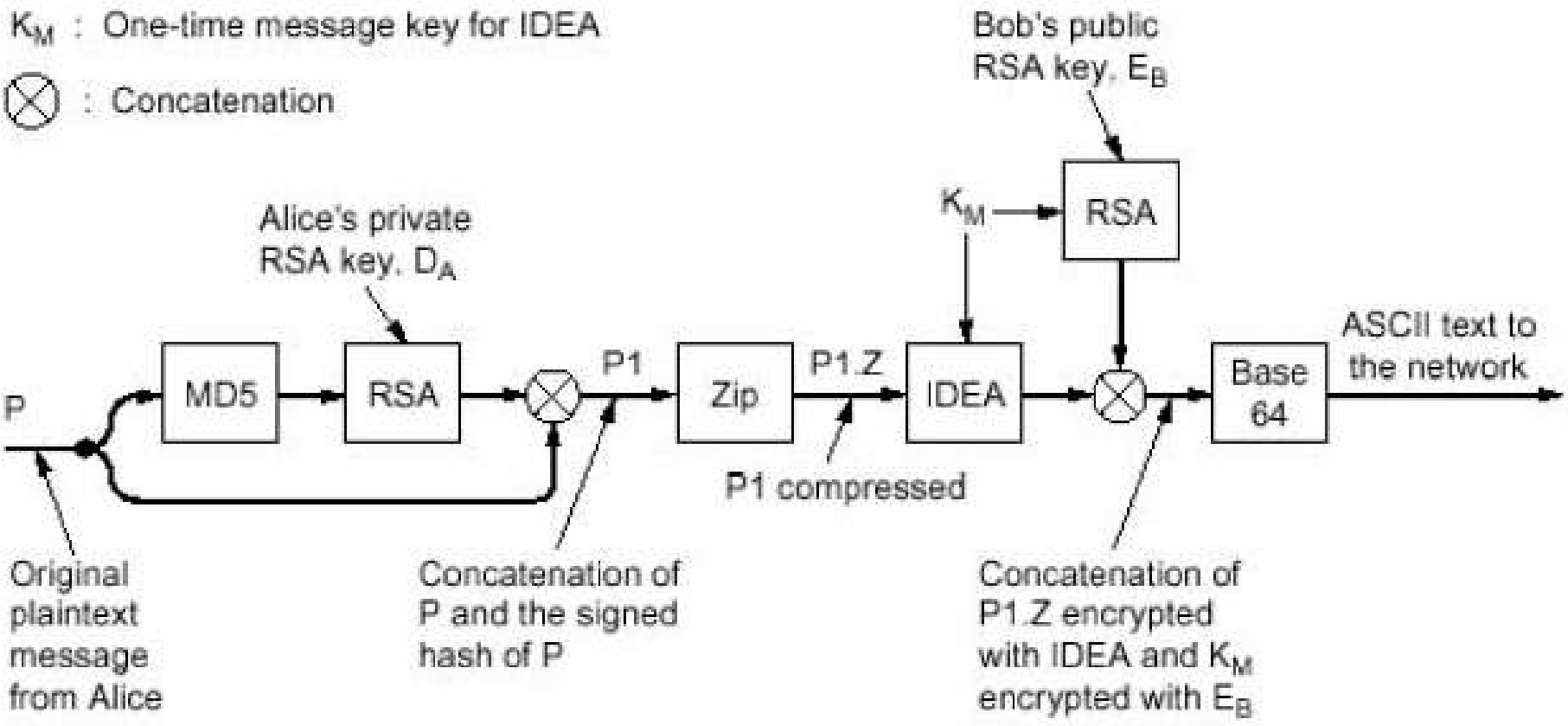
Using public keys



PGP – Pretty Good Privacy

- Secure e-mail system
  - Digital signatures
  - Compression
  - Key management
- Note use of slow / secure keys for small / important data items
- Fast / less secure keys for bulk of message

PGP Example

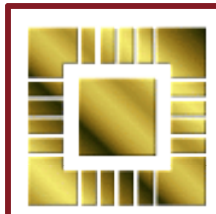

K_M : One-time message key for IDEA
: Concatenation
Bob's public RSA key, E_B
RSA
K_M
Alice's private RSA key, D_A
P
MD5
RSA
P1
Zip
P1.Z
IDEA
Base 64
ASCII text to the network
P1 compressed
Original plaintext message from Alice
Concatenation of P and the signed hash of P
Concatenation of P1.Z encrypted with IDEA and K_M encrypted with E_B

Secure Shell

- Replacement for Telnet & FTP
  - Can tunnel other protocols, e.g. X
- Authentication by RSA or passwords
- All communication encrypted
  - Choice of encryption algorithm
- Message integrity by MD5
- Random session keys, frequently changed

Security Principles

- Usually need to authenticate both parties
  - Not always, e.g. DNS updates
  - Time dimension: How long does authentication last?
- Use “permanent” secure keys (RSA) to send encrypted keys for faster, less secure encryption (DES, IDEA) but change frequently



Summary

- Understand examples of security systems
- How the tools / techniques used to build systems

- Remember
  - There is no single solution to “security”