Subject review: Outline

- **Revision**
- **Exam Format**
- What next?

Subject Outline

- This subject covers fundamental concepts in information security on the basis of methods from modern cryptography. We will concentrate on topics which are of current interest as well as the more `classic' topics which underlay this discipline.

- Topics drawn from:
  - symmetric key and public key cryptosystems,
  - hash functions,
  - authentication
  - secret sharing
  - Protocols
  - Key Management

- There will be some guest lectures in specialized topics.

Subject Description

- The objective of this subject is for students
- to understand the fundamentals of security principles in modern networks and computer systems,
- to be able to explain the protocols which ensure security in contemporary networked computer systems;
- to study various cryptographic primitives like encryption, hashing and signature functions which are used in theory and practice of network security.

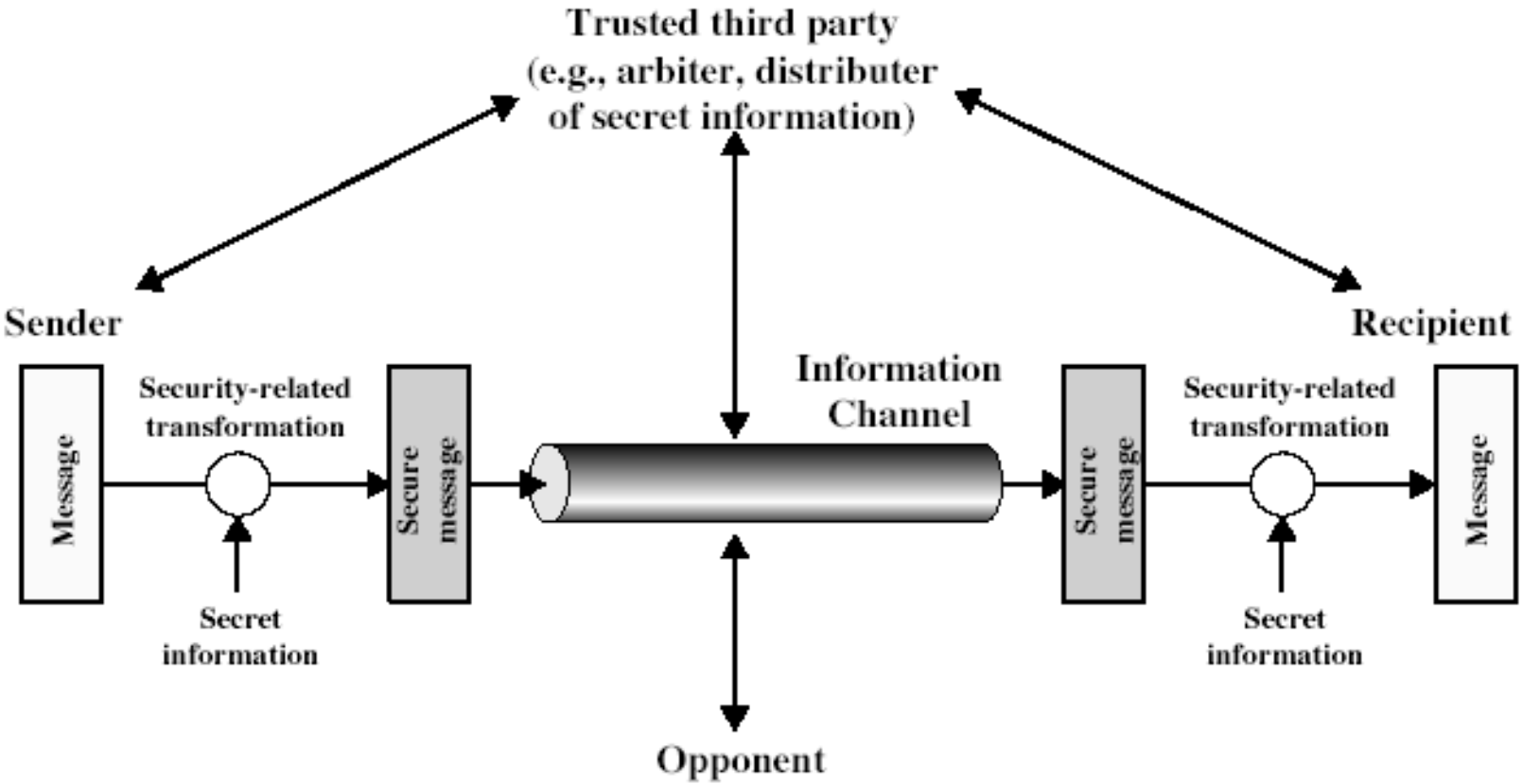
Course Plan (Dates to be Confirmed)

- Topics by week:
  - 1. Introduction to Security (Ch 1)
  - 2. Symmetric Ciphers,Block and Stream Ciphers (Ch 2,3,6,7) (Assignment 1 handed out)
  - 3. Basics from Number Theory (Ch 8) (Group Formation)
  - 4. Public Key Cryptography and RSA (Ch 9) (Assignment 1 due on Mon)
  - 5. Hash functions (Ch 11) (Project topics confirmation)(Assignment 2 handed out)
  - 6. Message Authentication Codes (Ch 12)
  - 7. Digital Signatures (Ch 13) (Assignment 2 due)
  - 8. Key management, (Mid Semester Test)
  - 9. Key management cont., Secret Sharing (Ch 14)
  - 10. Application/Advanced Topics (Part 5)
  - 11 Guest Lecture/Preparation for Project Presentations
  - 12.Review, Project presentations/ Report Due

Week 1

- Security Policy: Implementation and Mechanism aspects of Information Security.
- Three important concerns of Information security: CIA
- OSI Security Architecture:
  - Security attacks, Security Mechanisms, Security services.
- Model for Network Access Security
-

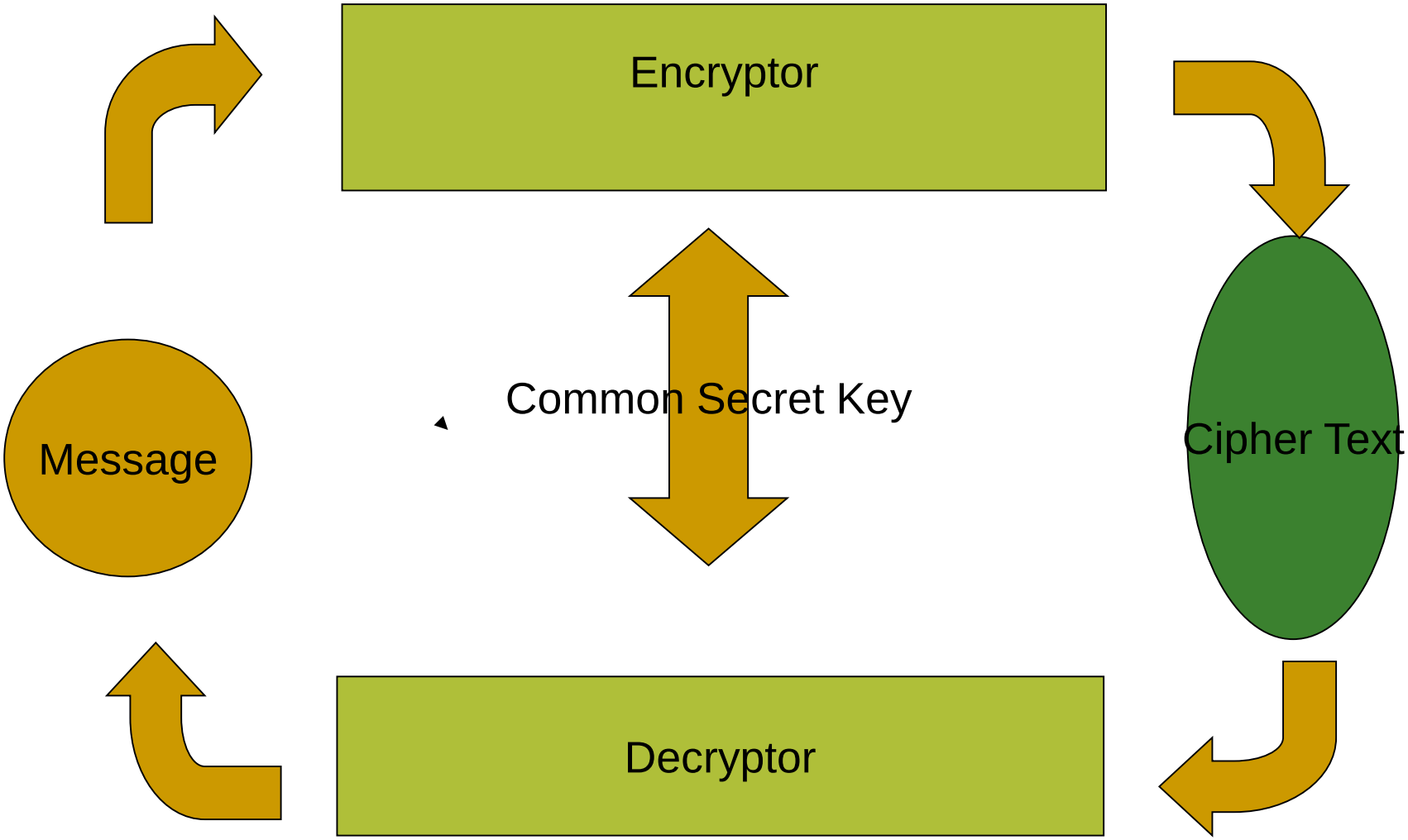
Model for Network Security



Week 2:Symmetric key Cryptography

- What are the two requirements for secure use of symmetric encryption?
- What is the main objective in the crypt analysis of symmetric key ciphers?.
- Definitions of Security.
- Classical Ciphers

Symmetric Key Cryptography



Block diagram of a Symmetric Key System: Logical view

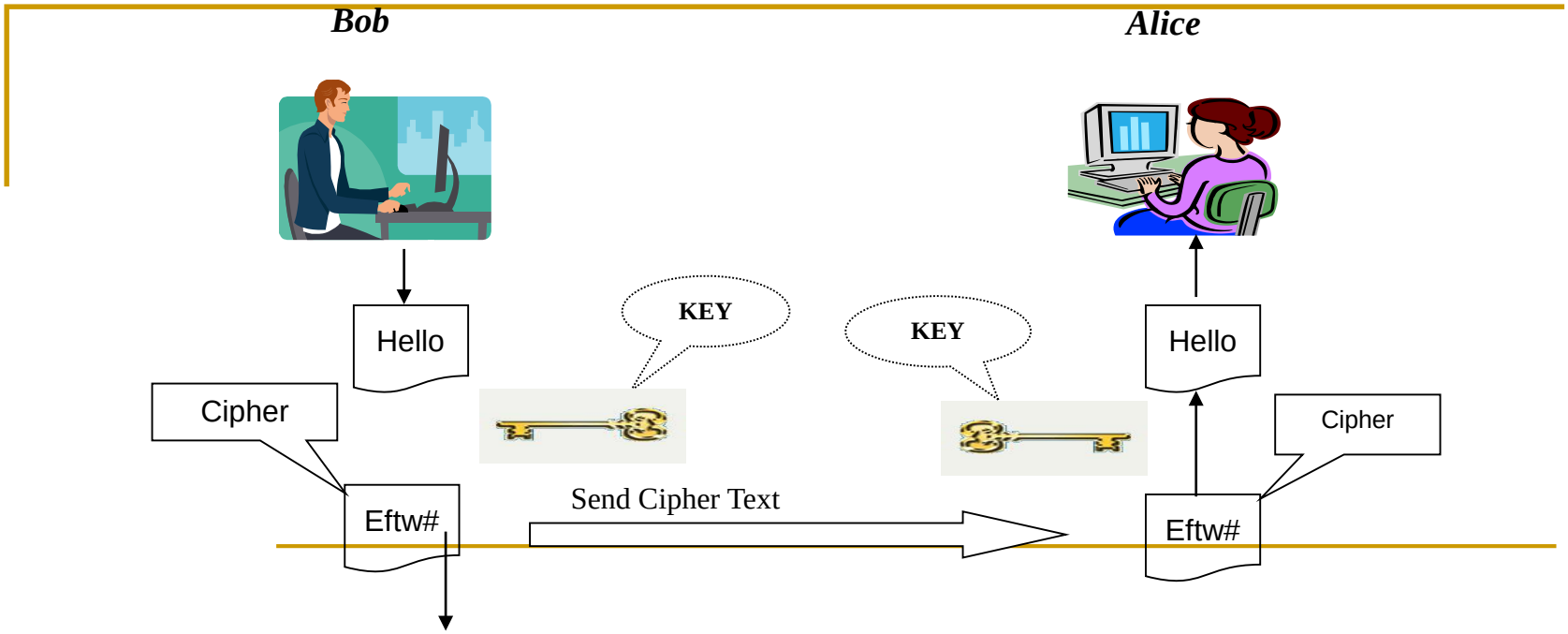
Week 3 :Block Ciphers

- Perfect Secrecy : One time pad
- Computationally Secure Ciphers
- Product Ciphers and Fiestel Ciphers
- Block Cipher Modes
  - Refer to Assignment 1 question

Week 4: Public Key Ciphers

- Some basic facts about numbers, Euler's theorem, Fermat's theorem, fields and rings.
- State the underlying intractable (hard) problems on which RSA cryptosystem is defined.
  - RSA problem
  - Factoring large integers.
- Diffie-Hellman problem

Limitations of Classical or traditional (Symmetric key) cryptography



Fast; Built-in Authentication; But, they need to share the key.

Confidentiality, but cannot protect against each other.

Man in the middle Attack

- Alice
- Choose Na
- g^{Na}

Malice

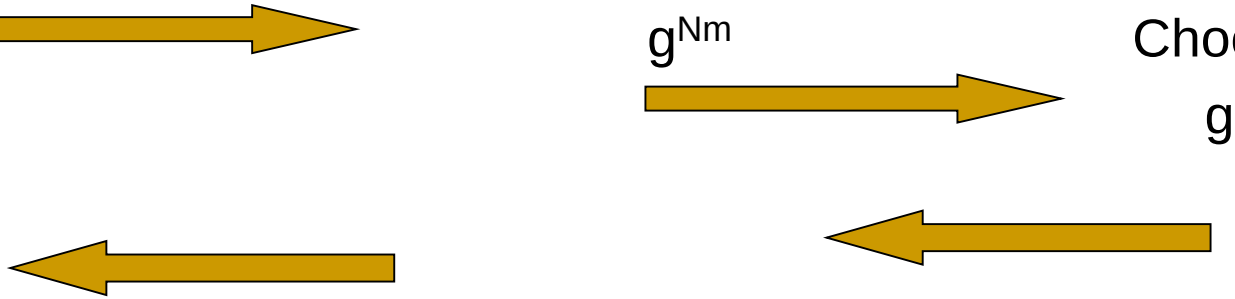
Choose Nm

g^{Nm}

Bob

Choose N_b

g^{Nb}



Gets g^{Nm}

Computes $(g^{Nm})^{Na}$

Computes $(g^{Nm})^{Nb}$

Malice shares k1= $g^{(Nm\ Na)}$ with Alice

Malice shares k2= $g^{(Nm\ Nb)}$ with Bob

Week 5: Hash Functions

- Definition and requirements.
- What is one-way property?
- What is collision-free property?
- How do you employ hash function for
  - Message integrity?
  - Message Authentication?
- What is birthday attack?

Birthday Attacks

- might think a 64-bit hash is secure
- but by **Birthday Paradox** is not
- **birthday attack** works thus:
  - given user prepared to sign a valid message x
  - opponent generates $2^{m/2}$ variations x' of x, all with essentially the same meaning, and saves them
  - opponent generates $2^{m/2}$ variations y' of a desired fraudulent message y
  - two sets of messages are compared to find pair with same hash (probability > 0.5 by birthday paradox)
  - have user sign the valid message, then substitute the forgery which will have a valid signature
- conclusion is that need to use larger MAC/hash

Week 6: Message Authentication Codes(MAC) and Digital Signatures

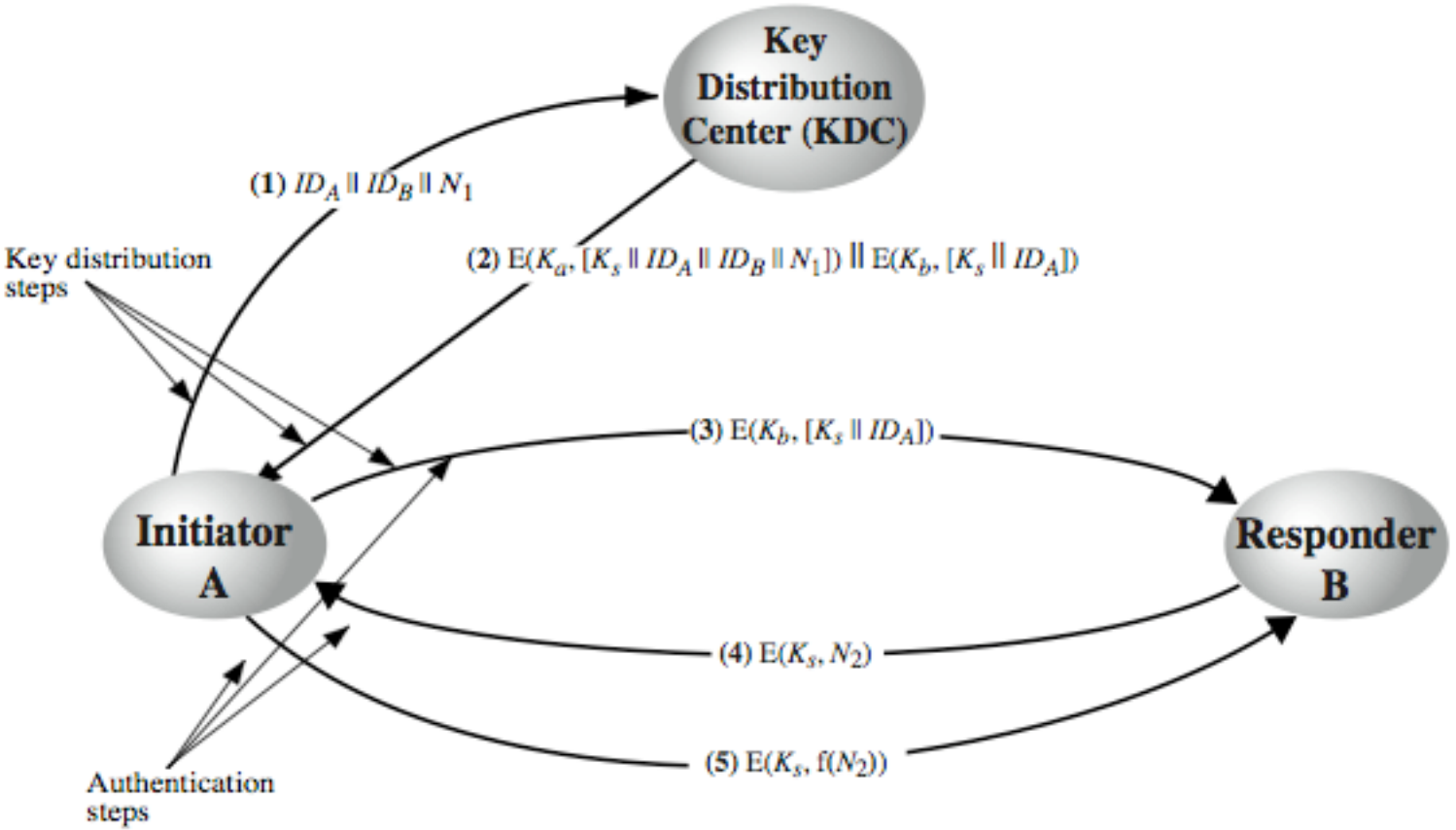
- Definition and requirements.
- How do you employ MAC function for
  - Message integrity?
  - Message Authentication?
- RSA as Digital Signatures
- What is the difference between MAC and Digital Signatures?

Week 7: Key Management 1

- What is the difference between link and end-to-end encryption?

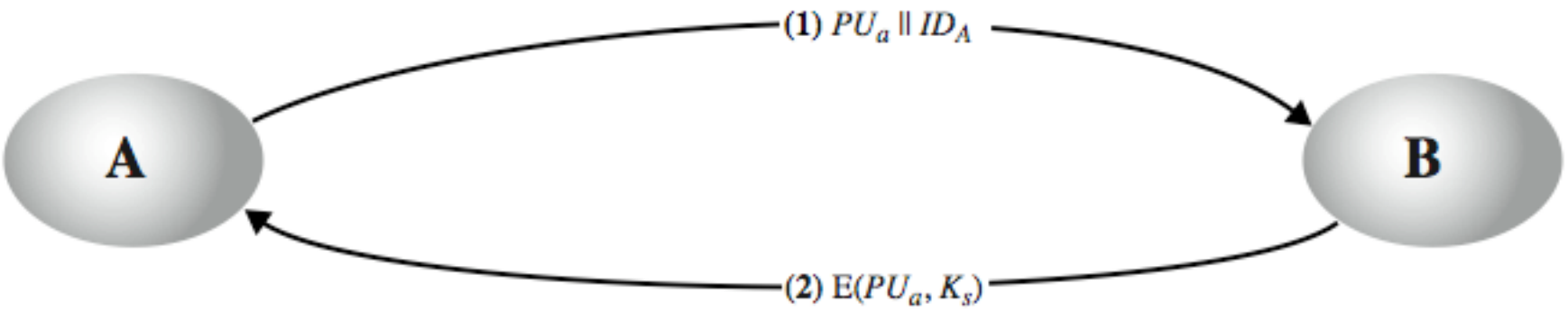
- Key Management for Symmetric Key Cryptography.
- Master and Session Keys.
- Discuss the Key Distribution Scenario.
- Symmetric Key Distribution using Public Key Encryption.

Key Distribution Scenario



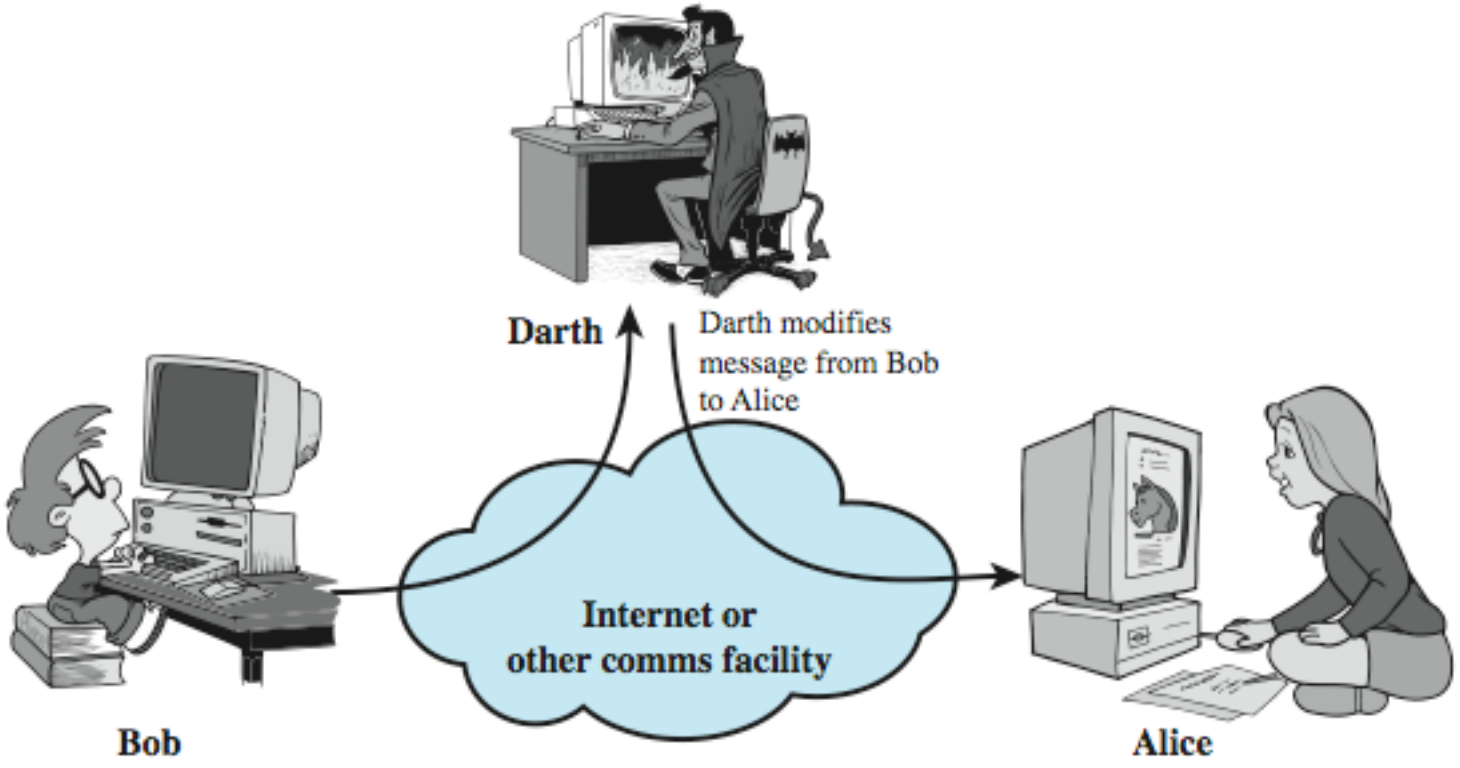
Simple Secret Key Distribution

- Merkle proposed this very simple scheme
  - allows secure communications
  - no keys before/after exist

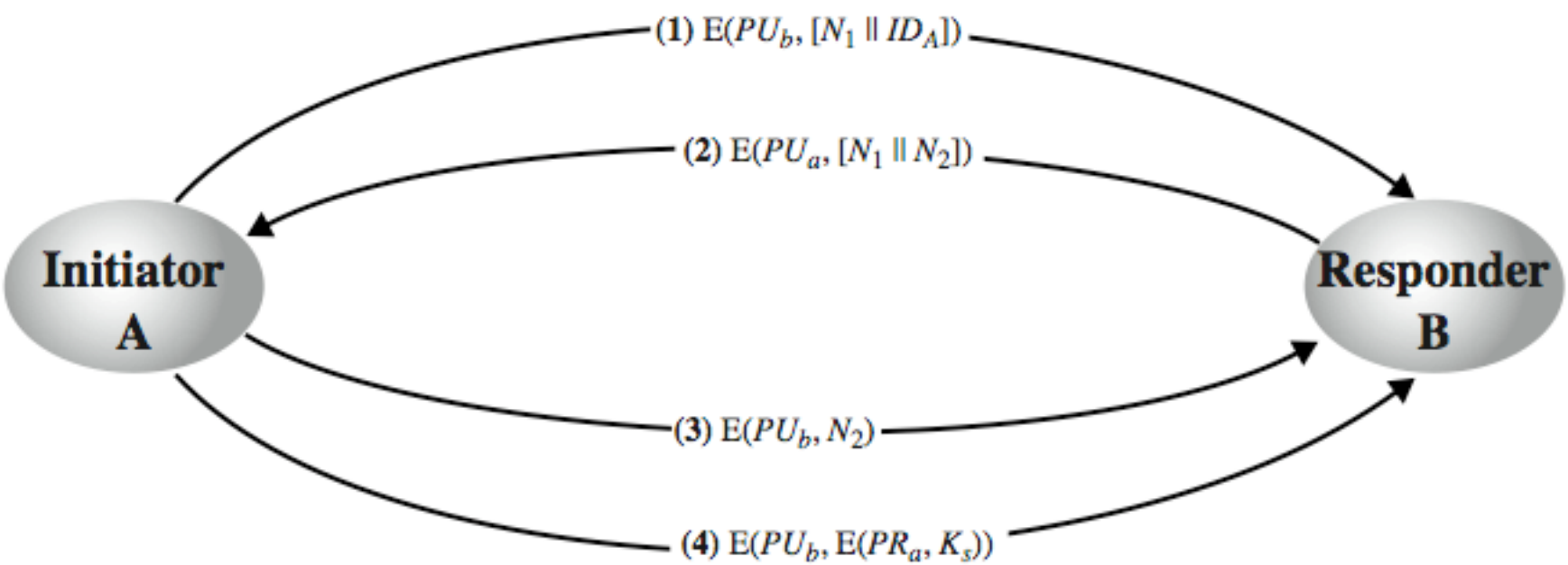


Man-in-the-Middle Attack

- this very simple scheme is vulnerable to an active man-in-the-middle attack



Secret Key Distribution with Confidentiality and Authentication



Week 8: Key Management 2

- Describe the four ways of distribution of Public Keys:
  - public announcement
  - publicly available directory
  - public-key authority
  - public-key certificates
- Public-Key Authority.
- Public Key Certificates and Revocation.

Week 9: Authentication

- What are the four means of authenticating user's identity?
  - based one something the individual
    - knows - e.g. password, PIN
    - possesses - e.g. key, token, smartcard
    - is (static biometrics) - e.g. fingerprint, retina
    - does (dynamic biometrics) - e.g. voice, sign
- Needham-Schroeder Protocol.
- Replay attacks.

Week 10: **KerberoS+SSL**

- What is Kerberos?
- What are its requirements?
  - Secure-prevent impersonation
  - Reliable-highly reliable and should employ distributed server architecture
  - Transparent-user should not be aware of the authentication process beyond the requirement to present a password.
  - Scalable-System should support large number of clients and servers.

- What are two important SSL concepts?.
  - SSL Connection and SSL Session:

Week 11: **Termpaper Presentations**

- What was important about the presentations and written reports ?
  - Experience in conducting research
  - Formulating coherent research topic.
  - Integrative writing - bringing together multiple aspects of a technology
  - Critical evaluation of techniques.

Week 12: **Review**

- "Generic skills" to take away from this course:
  - Ability to undertake problem identification, formulation, and solution
  - Ability to utilise a systems approach to complex problems and to design for operational performance
  - Ability to manage information and documentation
  - Capacity for creativity and innovation
  - Ability to communicate effectively, with the engineering team and with the community at large

Exam Format

- **See LMS pages on Exam Information**
  - Practice Exam.
  - Examinable Content.
  - Exam Details: Format and Venue.
    - See your timetable
      - Reading time is 15 minutes, so come early.
      - Writing time 2 hours
    - Venue: See the timetable
  - Exam Consultations:
    - I will update closer to the exam date.

What next?

- **You may like to consider doing advanced courses from mathematics.**
- **Consider doing research on Security related topics.**