SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience

Introduction to Cryptography

Lecture nineteen

Outline and learning goals of Lecture

- Secure communications
- Goals of cryptography
- Applications

References

- Hellman, Martin, “An overview of public key cryptography,” IEEE Communications, Vol. 16, Number 6, Nov. 1978 http://www.comsoc.org/livepubs/ci1/public/anniv/pdfs/hellman.pdf
  - The article that first brought public key encryption to a wide audience (published in a commemorative edition of IEEE Communications Magazine)
- Trappe, Wade and Washington, Lawrence, “Introduction to Cryptography with Coding Theory,” 2nd Edition
  - A very readable text with good coverage of modern crypto techniques
- Schneir, Bruce, “Applied Cryptography : protocols, algorithms and source code in C,” Wiley, 2nd Edition
  - The classic textbook on cryptography. A little dated now, but a very readable and at the same time comprehensive text on crypto foundations and algorithms

From Bruce Schneier

From the preface of “Applied Cryptography”

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister reading your files, and cryptography that will stop major governments reading your files. This book is about the latter.

“If I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to try and read the letter, that’s not security. That’s obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and world’s best safecrackers can study the locking mechanism – and you still can’t open the safe and read the letter – that’s security.”

Cryptography basics

- Sender and receiver
- Plaintext and cipher text
  - Unencrypted and encrypted message
- Encryption and decryption
- Cryptology
  - Mathematics and study of cryptography
- Cryptanalysis
  - Breaking of cipher texts

Cryptography basics

- At the heart of cryptography is the aim of changing ordered data into a seemingly random string
- Only by knowing the key or keys can the data be encrypted and decrypted
- Cryptography covers more than confidentiality
  - Enables authentication, integrity, non-repudiation
- Cryptosystem
  - Comprised of:
    - Software
    - Protocols
    - Algorithms
    - Keys

Persona traditionally used in cryptography

- Sender is usually Alice
- Receiver is usually Bob
- Other parties to the communication may be Carol and Dave
- An eavesdropper is usually Eve
- Mallory may be a malevolent eavesdropper
- Oscar is an opponent (not necessarily malevolent)
- A trusted arbitrator is usually Trent
- A warden who may police communications is Walter or Wendy

Cryptography terminology

- Plain text
  - The unencrypted message
- Cipher text
  - The message after encryption
- Key
  - The information needed to decrypt or encrypt the message
- Key space
  - Range of values that can be used to construct the key
- The algorithm
  - Rules used for encrypting and decrypting the message

Kerkhoff's Principle

- Expressed in 1883
  - The number of secrets needed in a cryptosystem should be kept to a minimum
- Should the algorithm used in a cryptosystem be made public?
  - Kerkhoff's principle states that it should
  - The only thing that a cryptosystem should rely on for security is its key
  - By making the algorithm public and letting anyone attempt to compromise the cryptosystem, its security can be tested
- Not always accepted
  - Many governments dislike the idea of publicising their algorithms
  - Prefer the risk of an error to the sustained scrutiny publication brings
- Commercial enterprises generally adopt Kerkhoff's principle

Strength of cryptosystems

- A number of factors that affect the strength of cryptosystems
- The algorithm
  - Block algorithms consist of rounds of substitution and permutation. An algorithm might be compromised if it doesn't use enough (a weakness in some implementations of RC5)
  - An ideal stream cypher should map input values randomly across the entire cipher space. Some algorithms have biases where a subset of the cipher space is mapped more commonly than others (a weakness of RC4)
- The length of the key
  - Generally, the longer the key, the greater the strength of the cryptosystem

Strength of cryptosystems

- The secrecy of the key
  - All cryptosystems rely on a secret key of some sort. If secrecy of the key is compromised (for example by protecting it with a weak password) then the cryptosystem is compromised
- Initialisation vectors
  - Do not want the same sequence mapped to the same cipher text for every message
  - Usually prevented by ‘starting’ the cryptosystem with a different set of values (‘nonces’)
  - Initialisation vectors need to be different each time used
- Configuration within a cryptosystem
  - For example does the system have secure exchange of symmetric keys, does it make use of session keys?

Strength of cryptosystems

- Usually expressed in terms of average length of time with available computing power needed to find the correct key to decrypt a message
- Strength of a cryptosystem is not just dependent on key
  - Weak keys, algorithmic flaws, dependence on passwords
- Appropriate strength for a cryptosystem depends on its purpose – security policy

Government restrictions on cryptography

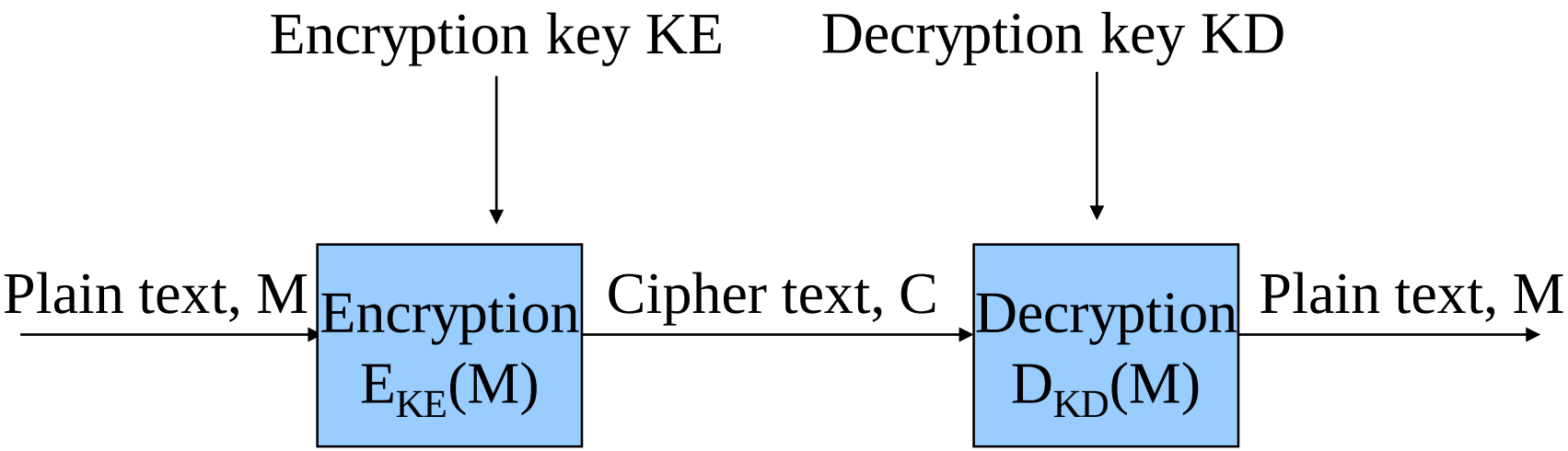
- The United States has been very antagonistic to the export of cryptosystems including algorithms
  - Have not supported Kerkchoff's principle
- Very heavily regulated from the 60s to the 80s
- Cryptosystems designated 'armaments' and subject to similar controls
- Caused considerable conflict between government and researchers, business and communications companies
- Prohibited export of equipment (including algorithms and software that included
  - Symmetric algorithms with keys greater than 56 bits
  - Asymmetric algorithms with keys greater than 512 bits or 112 bits (depending on type of algorithm)

Services that can be provided through cryptography

- Secure communications
- Integrity
  - Ensuring messages from Alice have not been altered, intentionally or unintentionally
- Authentication
  - Proof that the party sending the message is Alice
- Non-repudiation
  - Ability of Bob to prove to a third party Trent that the message did come from Alice
- Note the distinction between Authentication and Non-repudiation

Secure communications

- Process of converting a plaintext message to ciphertext using a pre-arranged method
- Usually assumed that attackers know the method. Secrecy based on the key
- Alice encrypts the message with an encryption key. Bob decrypts it with a decryption key



Attacking secure communications

- Eavesdropper Eve may have the following goals as regards the secure communications
  - Read the message
  - Find the decryption key and so be able to read all messages from Alice
  - Corrupt Alice's message so Bob will think Alice sent the altered message
  - Masquerade as Alice and so communicate with Bob, so that Bob thinks he is communicating with Alice

Possible attacks

- Ciphertext only
  - Eve has only a copy of the ciphertext
- Known plaintext
  - Eve has a copy of the cipher text and the corresponding plaintext
- Chosen plaintext
  - Eve gains temporary access to the encryption machine. She cannot open it to determine the key but can use it to encrypt chosen plaintext messages and so hope to determine the key that way
- Chosen cipher text
  - Eve gains temporary access to the machine. Again, she cannot determine the key directly from her access, but can use it to decrypt chosen cipher text messages and hope to determine the key that way

Importance of key length

- Simplest attack on a cryptosystem is to try every key until one is found
  - "Brute force" attack
  - On average, if there are N possible keys a bruteforce attack will require N/2 attempts to find the correct key
- The number of possible keys depends on the key length
  - If there are k bits in the key, the number of possible keys is usually $N = 2^k$
    - (A famous exception is DES. DES key length is 64 bits but 8 bits are parity so number of keys is 2^{54})
  - The longer the keylength, the slower a bruteforce attack

‘Breaking’ of a cryptosystem

- ‘Breaking’ is a misleading term
  - Implies the cryptosystem is no longer usable
    - Not true
- ‘Breaking’ means that weaknesses in the cryptosystem have been found that enable **some** messages using **some** keys to be decrypted more quickly than bruteforce
  - ‘breaking’ can mean a speed-up in an attack time when compared with bruteforce (say 10,000 times).
  - But if a bruteforce attack would take millions of years (with existing equipment) then a 10,000 time speed-up is not that useful
- ‘Broken’ systems can often be made quite secure with regular key changes

Symmetric and asymmetric algorithms

- There are two broad categories of cryptographic methods
  - Symmetric key and asymmetric key
- Classical (pre 1970) cryptographic methods are all symmetric key
  - The same key is used to both encrypt and decrypt (possibly with some simple modification)
  - DES, AES, RC4 are perhaps the most well known and widely implemented algorithms
- Public key algorithms introduced in the 70s revolutionised cryptography
  - Different key used for encryption and decryption.
  - Knowing one key tells you nothing about the other key
  - RSA, El-Gamal, elliptic curve best known examples

Symmetric key cryptography

$E_k(M) = C$

encryption

$D_k(C) = M$

decryption

K encryption and decryption key

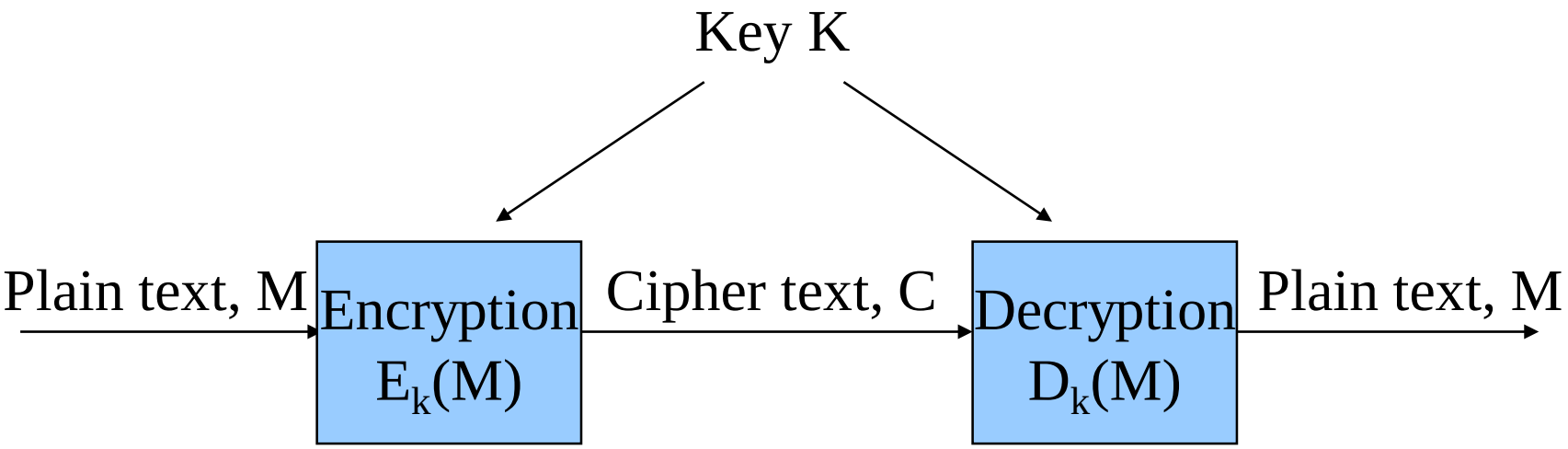
M plaintext

C ciphertext

$D_k(E_k(M)) = M$

Converse not necessarily true

Symmetric key cryptography



Symmetric key cryptography

- Advantages
  - Most common symmetric key algorithms are very fast
    - Algorithms require a small number of operations and a small amount of information kept in memory
    - Lends themselves to hardware implementation
  - Can provide confidentiality, authentication and integrity
- Disadvantages
  - Key distribution
    - Large number of keys needed
  - Difficult to provide non-repudiation

Questions to illustrate key explosion

- Suppose your organisation has 20 people in it. Each of them may wish to communicate with each of the other 19 people. Each of them wish their communications to be confidential, that is no one other than the recipient should be able to decode the cipher text.
  - How many keys does each person need to keep secret?
  - How many keys in total?
- Suppose your organisation has 10 people in it. Despite being such a small organisation it is faction ridden. Factions may consist of 2, 3 or 4 people. Individuals may belong to more than one faction. Each faction has its own secret key. How many possible secret keys?

Public key cryptography

- Sometimes Asymmetric cryptography
- Examples are RSA, Elliptic curve algorithms
- Sender and receiver use different keys for encryption and decryption
  - a key pair
- Key pairs are mathematically dependent
  - message encrypted by one key can only be decrypted using the other key of the key pair
  - But knowledge of one key tells you nothing about the other key
    - It is impossible (or very very difficult) to derive the private key from the public key

Public key cryptography

- Anybody can encrypt with the public key but only the holder of the private key can decrypt it
- The holder of the private key can encrypt a message that anyone can decrypt with the public key
- Enables
  - Confidentiality (Usually used for key distribution)
  - Authentication
  - Non-repudiation
  - Solves the key explosion problem

  BUT
  - Much slower (1000s of times) than symmetric key algorithms
  - Key lengths much longer (10s) than symmetric key algorithms for same level of security

Public key cryptography

$E_{k1}(M) = C$

$D_{k2}(C) = M$

K1 = encryption key

K2 = decryption key

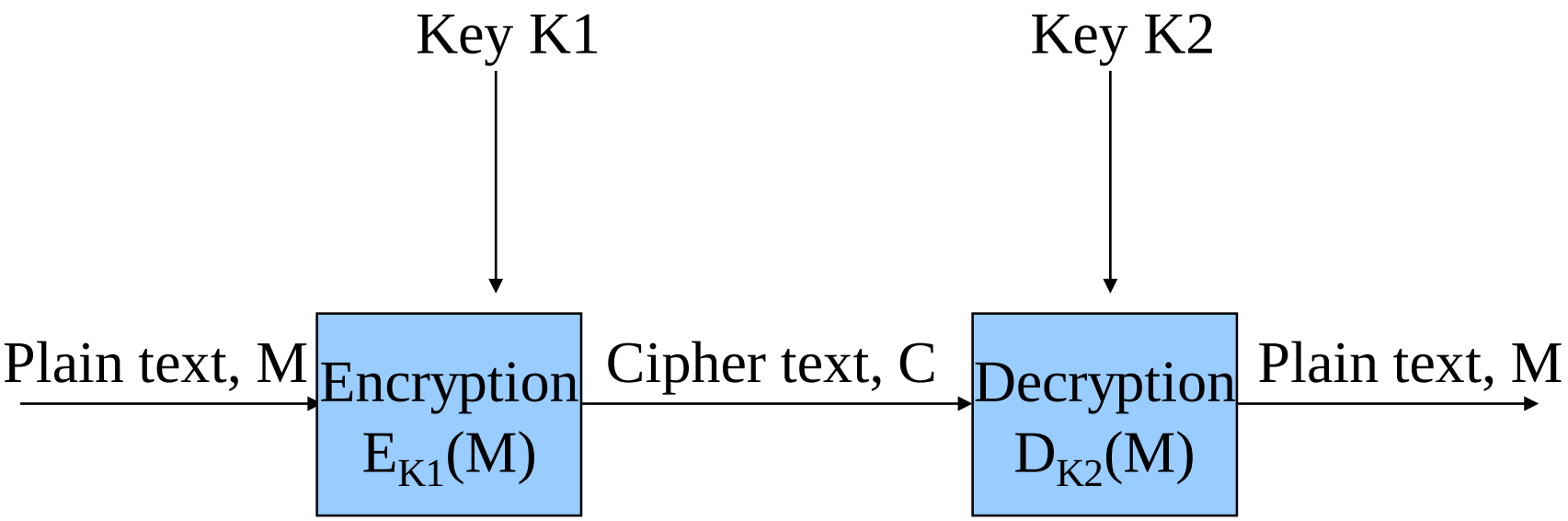
M plaintext

C cipher text

$D_{k2}(E_{k1}(M)) = M$

Converse is usually true

Public key cryptography



Public key cryptography services

- Confidentiality
  - Alice wishes to send a message to Bob that is to be kept secret. She encrypts the message with Bob's public key. Bob decrypts it with his private key
  - Public key cryptography is usually not used for confidentiality of messages. Too slow. But can be used to exchange symmetric keys
- Authentication
  - Alice wishes to authenticate her identity to Bob. Knowing the private key associated with Alice's public key is proof of identity
  - Bob sends a challenge to Alice. Alice encrypts the challenge with her private key and sends it to Bob. Bob decrypts the response with Alice's public key. If the decrypted response matches the challenge Alice's identity is proven

Public key cryptography services

- Integrity
  - Bob downloads software that Alice has digitally signed. Bob trusts Alice to verify the software. Bob verifies Alice's digital signature by using Alice's public key.
- Non repudiation
  - Bob wishes to prove to Trent that Alice really did send a particular message that Alice signed. Bob forwards the message to Trent. Trent verifies Alice's digital signature on the document using Alice's public key.

Public key cryptography

- Advantage of public key cryptography compared with symmetric key cryptography is that no confidential information need be exchanged before communication takes place
  - Can provide a secure but open communication channel for exchange of symmetric keys
  - Can also be used for authentication, integrity and non-repudiation
  - Public key can be very public
    - attached to emails
    - located in register
    - on web pages
    - transmitted in plaintext as part of protocol exchange (eg SSL)

Public key cryptosystems

- Rivest – Shamir – Adleman (RSA)
  - Based on factoring of 100 to 200 digit prime numbers
  - Easy to multiply and calculate products of large numbers
  - very difficult to factor a large number you know to be the product of two prime numbers
- Public key algorithms are rarely used to encrypt user data or messages.
  - Used to encrypt session keys which are then used to encrypt user data
  - Used for authentication and non-repudiation
  - TLS / SSL

Examples of applications of public key cryptosystems

- Key exchange
- Proof of identity
- Onion routing
  - We will discuss all these later
- Non repudiation
  - Provided through digital signatures
- Many of the services are provided through digital signatures
  - Digital signatures rely on hashes

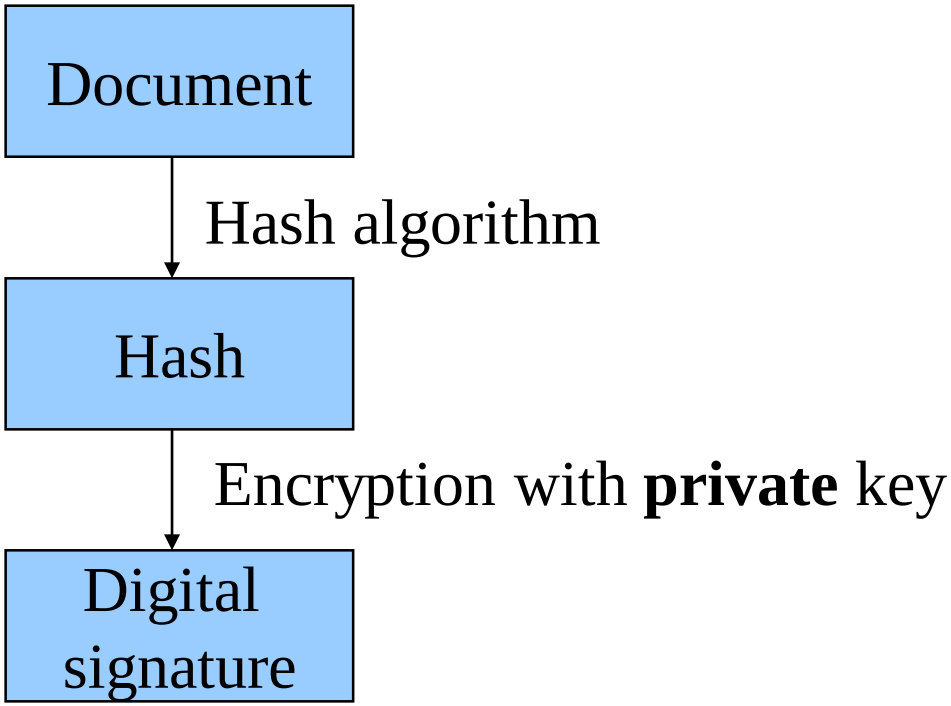
Hashes (recap)

- One-Way Function with special properties
- Convert an indeterminate size block of data to a small, fixed-length output
  - All output values generated with equal probability
  - Single bit change in input => large and indeterminate change in output
  - Difficult to generate a document that hashes to a particular value
- Protects against tampering – provides detection
- Enables authentication and non-repudiation
- Popular hashes: MD5, SHA-1, SHA-256

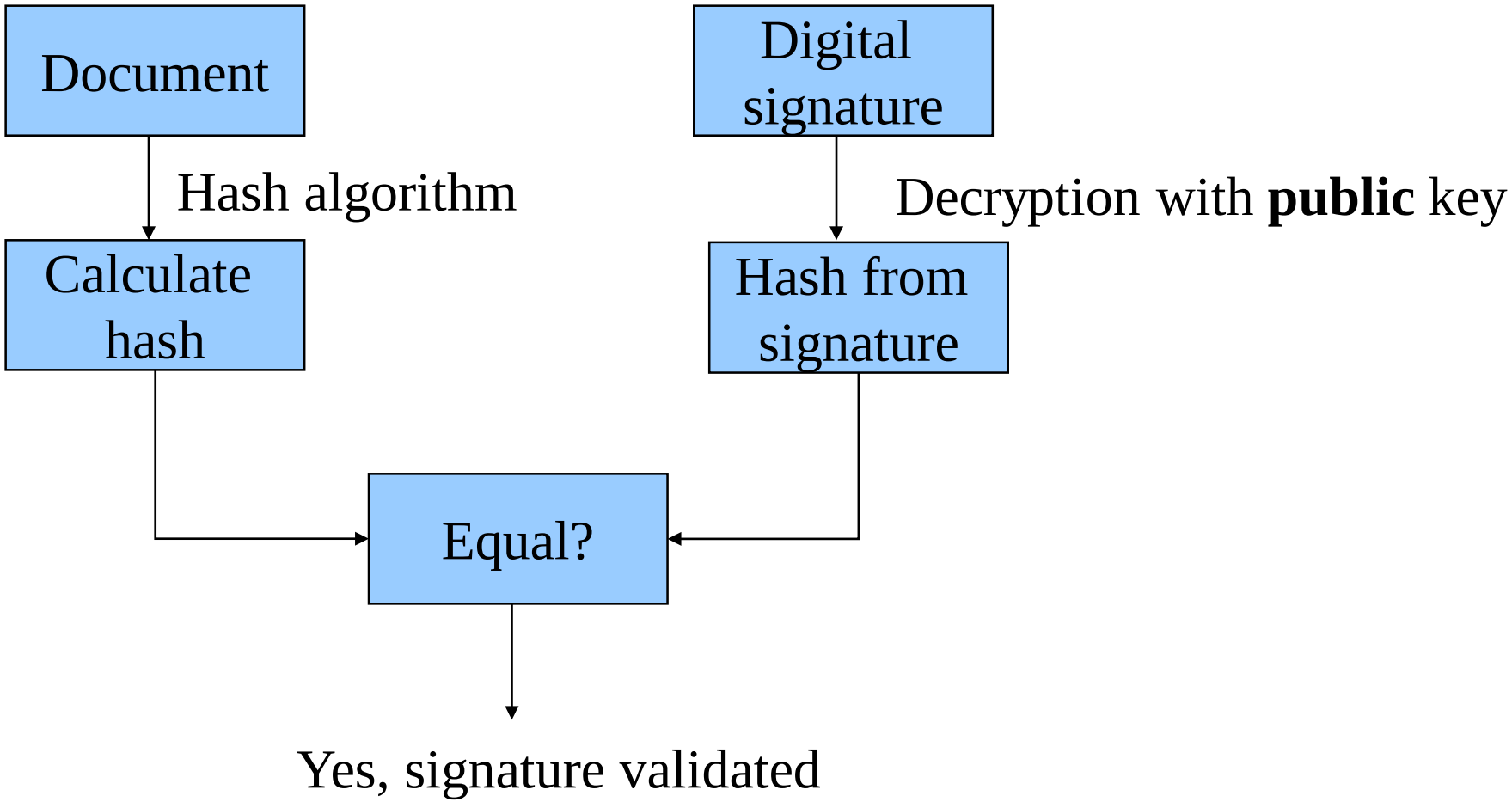
Public Key – Signing & Authentication

- Public keys and hash algorithms allows signing of digital documents
  - An electronic document can be signed
    - A hash of the document is calculated
    - The hash is **encrypted** with a **private** key
    - A third party can later recompute the hash, decrypt the encoded hash using a **public** key, and compare
    - Document is protected by hash within signature
  - Better than written – private key cannot be forged
  - If confidentiality is required, it can also be encrypted
  - Can use known public keys to authenticate signatures

Digital signature construction



Digital signature validation



Public Key – Non-repudiation

- Non-repudiation
  - Ensures that a party to a digital transaction cannot repudiate the transaction (claim that it did not take place)
  - Protects other parties to contracts
  - Protects commercial interests
- Different to authentication
  - Authentication can be provided using symmetric cryptography
  - Knowledge of a shared secret key is proof of identity
  - Non repudiation not possible with symmetric cryptography
  - Bob (recipient) could forge a message using the shared secret
  - Since only Alice knows her private key, no one else can forge her signature on a digital document

Symmetric and Public Key Cryptography

- Symmetric Key Cryptography
  - Same key used to both encrypt and decrypt data
  - Key must be known only by communicating parties
  - Traditional view of cryptography
  - Most commonly known ciphers
    - DES
    - RC4
    - AES
- Public Key Cryptography
  - Pair of keys: Ka and Kb
    - Encrypt with K_a, must decrypt with K_b
    - Encrypt with K_b, must decrypt with K_a
  - One key is made public whilst the other is private
  - Most commonly known ciphers
    - RSA
    - Elliptic curve cryptography

Symmetric and Public Key Cryptography

- Symmetric Key Cryptography
  - Encryption algorithm very fast – can process data at a higher rate
  - Key Length is shorter for same amount of security compared with asymmetric key cryptography
- Public Key Cryptography
  - Algorithm is much slower due to complexity
  - Longer Key Length generally required for same degree of security as symmetric key cryptography

Symmetric and Public Key Cryptography

- Symmetric Key cryptography
  - Used for confidentiality and authentication
  - Does not provide non-repudiation
  - Does not allow digital signing
- Public Key Cryptography
  - Mainly used for key distribution, authentication and non-repudiation.
  - Enables secure communications between unknown and untrusted parties
  - Supports authentication, non-repudiation and digital signing
  - Secure delivery to one person or all (tamper proof)

Summary

- Introduction to cryptography
- Attacks on cryptosystems
- Role of symmetric and asymmetric encryption in providing
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Authentication