

Encryption

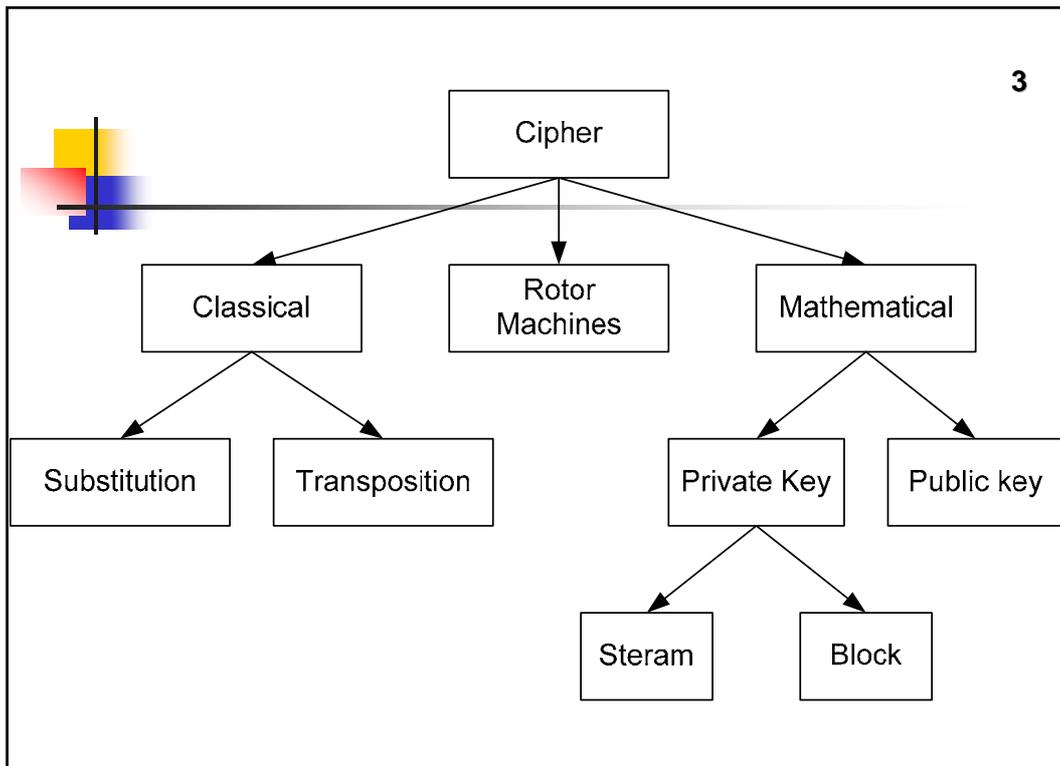
Mathematical methods

Dr.Talal Alkharobi

2

Encryption secrecy

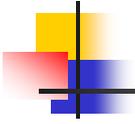
- It was finally recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible, nor practical, safeguard;
- In fact, any adequate cryptographic scheme should remain secure even if the adversary knows the cipher algorithm itself.
- Secrecy of the key should alone be sufficient for confidentiality when under attack — for good ciphers.
- This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called Kerckhoffs' principle;
- Alternatively and more bluntly, it was restated by Claude Shannon as Shannon's Maxim — 'the enemy knows the system'.



4

Private-Key Cryptography Symmetric-key

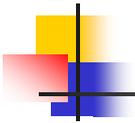
- A class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption.
- The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys.
- The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private link.
- Other terms for symmetric-key encryption are single-key, one-key and private-key encryption.



Private-Key Cryptography Symmetric-key

5

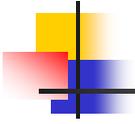
- Symmetric-key algorithms are not always used alone.
- In modern cryptosystem designs, both asymmetric (public key) and symmetric algorithms are used to take advantage of the virtues of both.
- Such systems include SSL, PGP and GPG, etc.
- Asymmetric key algorithms make key distribution for faster symmetric key algorithms.
- Some examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (aka Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA.



Private-Key Cryptography Symmetric-key

6

- Types of Symmetric-key algorithms can be divided into
 - Stream ciphers: encrypt the bits of the message one at a time, and.
 - Block ciphers: take a number of bits and encrypt them as a single unit



Private-Key Cryptography Symmetric-key

7

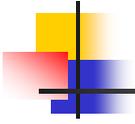
- Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms.
- In practice, this means that a quality asymmetric key algorithm is hundreds or thousands of times slower than a quality symmetric key algorithm.



Private-Key Cryptography Symmetric-key

8

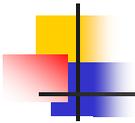
- Disadvantage: the requirement of a shared secret key, with one copy at each end.
- Since keys are subject to potential discovery by a cryptographic adversary, they need to be changed often and kept secure during distribution and in service.
- The consequent requirement to choose, distribute and store keys without error and without loss, known as key management, is difficult to reliably achieve.
- In order to ensure secure communications between everyone in a population of n people a total of $n(n - 1)/2$ keys are needed



Private-Key Cryptography Symmetric-key

9

- Very often these days, the much slower asymmetric algorithms are used to distribute symmetric-keys at the start of a session, then the higher speed symmetric-key algorithms take over (see Transport Layer Security).
- The same problems of reliable key distribution still exists at the asymmetric level, but they are somewhat more tractable.
- However, the symmetric key is nearly always generated in real-time.
- The symmetric-key algorithms can't be used for authentication or non-repudiation purposes; instead hash functions are commonly used



Private-Key Cryptography Symmetric-key

10

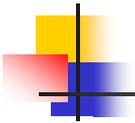
- Encryption functions must, by definition, be reversible since you need to be able to both encrypt and (provided you have the right key) decrypt messages.
- Various methods have been used historically to manage this.
 - Book ciphers, in which the shared key is related to some content in a book,
 - Auto-key ciphers in which the key is partially derived from the plaintext,
 - Grille ciphers in which each party has identical pieces of paper with holes cut out to lay over the base message in order to extract the encoded message



Public key cryptography Asymmetric

11

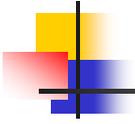
- A user has a pair of cryptographic keys - a public key and a private key.
- The private key is kept secret, while the public key may be widely distributed.
- The keys are related mathematically, but the private key cannot be practically derived from the public key.
- A message encrypted with the public key can be decrypted only with the corresponding private key.



Public key cryptography Asymmetric

12

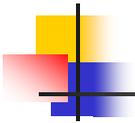
- The two main branches of public key cryptography are:
 - Public key encryption: used to ensure confidentiality
 - a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key
 - Digital signatures: used to ensure authenticity.
 - a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with.



Public key cryptography Asymmetric

13

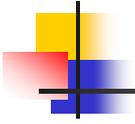
- An analogy for public-key encryption:
 - A locked mailbox with a mail slot.
 - The mail slot is exposed and accessible to the public
 - Anyone knowing the street address can drop message
 - Only the person who possesses the key can open the mailbox
- An analogy for digital signatures
 - The sealing of an envelope with a personal wax seal.
 - The message can be opened by anyone,
 - The presence of the seal authenticates the sender.



Public key cryptography Asymmetric

14

- A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party.
- The usual approach to this problem is to use a public-key infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify ownership of key pairs.
- Another approach, used by PGP, is the "web of trust" method to ensure authenticity of key pairs



Public key cryptography Asymmetric

15

- Public key techniques are much more computationally intensive than purely symmetric algorithms.
- The judicious use of these techniques enables a wide variety of applications.
- In practice, public key cryptography is used in combination with secret-key methods for efficiency reasons.
- For encryption, the message may be encrypted with secret-key algorithm using a randomly generated key, and that key encrypted with the user's public key.



Public key cryptography Asymmetric

16

- For digital signatures, a message is hashed (using a cryptographic hash function) and the smaller "hash value" is signed;
- before verifying the signature, the recipient computes the hash of the message himself, and compares this hash value with the signed hash value to check that the message has not been tampered with