Applied Cryptography Introduction Services and Processes

Cryptography One

Ed Crowley

Fall '08

Topics

- Introduction
  - Focus
  - Case Study
  - Definitions
- Services
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation
- Processes
  - Encryption
  - Hash Functions
  - Message Authentication
  - Digital Signatures

  Cryptography Evolution
- One Time Pad Cryptogram

Focus: Cryptographic Applications

Specifically, cryptographic applications that provide enterprise security services including:

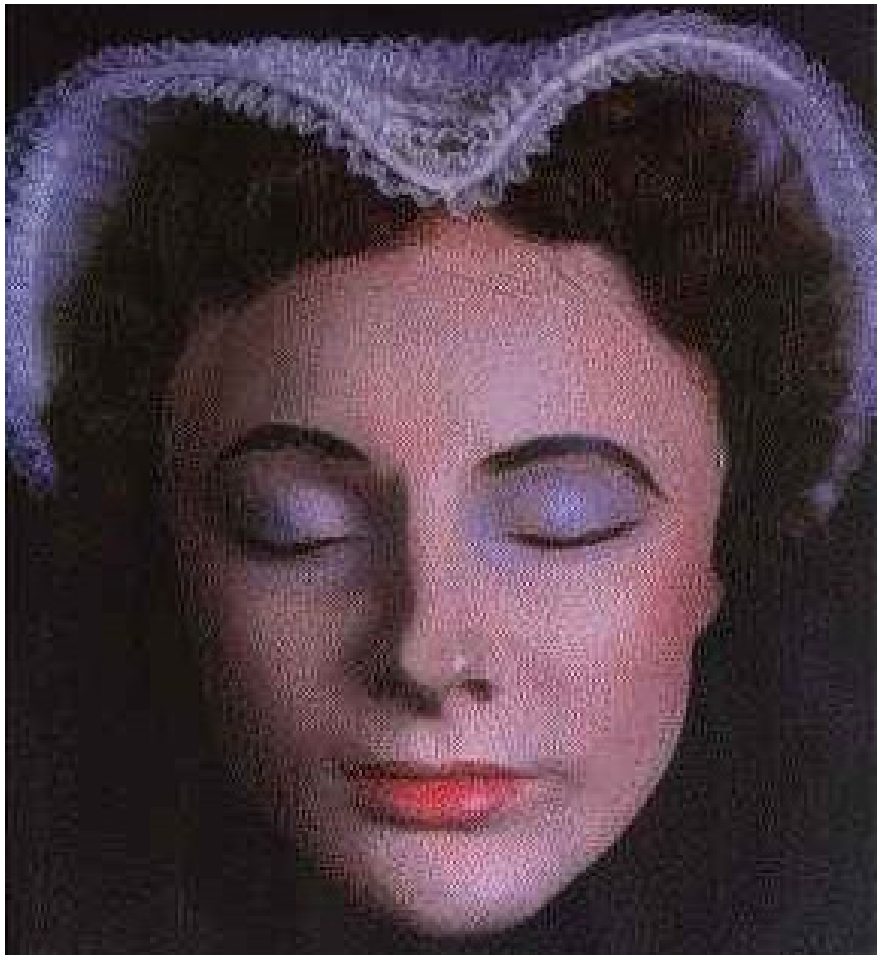
- Confidentiality
- Integrity
- Authentication
- Non-repudiation

- Basic crypto services prepare us to learn related technologies, methods, and mechanisms including:
  - Digital signatures
  - Secure protocols
  - Virtual Private Networks.

Goals

- Introduce crypto basics
- Facilitate the assessment and evaluation of cryptographic based enterprise security services.
- Lecture Modules
  1. Introduction to Cryptography: Services and Processes
  2. Cryptographic Technologies and Algorithms
  3. Key Management Problems and Cryptanalysis
  4. Public Key Infrastructure and Secure Protocols
  5. A Brief History of Cryptography including Related Terms

Why Learn Cryptography?



Mary Queen of Scots

1542 – 1587

An introduction to (mis)-applied cryptography.

Mary Queen of Scots

- Jan 1586, Mary, who was in prison, began to receive letters
  - Smuggled to her by Gilbert Gifford.
  - Letters enciphered with a nomenclator.
    - A nomenclator is somewhat analogous to a monalphabetic cipher with symbols replacing certain words.
- Letters were smuggled in a hollow beer bung.
  - Form of steganography
- Within the letters, what has become known as, the Babington Plot was proposed.

Babington Plot

- Involved Anthony Babington and a small group.

In essence, the plot proposed to:

1. Free Mary Queen of Scots
2. Assassinate Mary's Cousin Queen Elizabeth
3. Have Mary succeed Elizabeth as Queen of England.

- However, the plot had a few problems.
- Prominent among the probles was the mis-application of cryptography

Gilbert was a Double Agent

First, delivered letters to Queen Elizabeth's Secretary.

- Applied cryptanalysis.
  - Broke the code
  - Became aware of the plot.
- Later, the letters were delivered to the appropriate conspirators.

- To entrap the conspirators, the secretary forged a message postscript. In part, it read:

  I would be glad to know the names and qualities of the six gentlemen which are to accomplish the designment; for it may be that I shall be able …, to give you some further advice …

Five Observations

1. The nomenclature lacked authentication and non-repudiation.
2. When Gilbert turned out to be a double agent, steganography no longer kept the messages hidden.
3. When cryptanalysis was applied, confidentiality was lost.
4. When the opposition was able to add a post script, integrity was lost.
5. When the trial was over, Mary's head was lost!
   - If Mary would have understood cryptography better, she may have kept her head!

Cryptography Defined

- Original definitions sprang from its literal meaning, that is from the original Greek, (“kryptos” as “hidden” and “-graphy as “writing”.)

As technology evolved however, so did its definition. For example, the U.S. Army Field Manual FM 34-40-2 defines cryptology as

- “… the branch of knowledge which concerns secret communications in all its aspects.

- A more contemporary and complete definition, from NIST:

  “… a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, data integrity, authentication, authorization and non-repudiation.”

Cryptographic Services

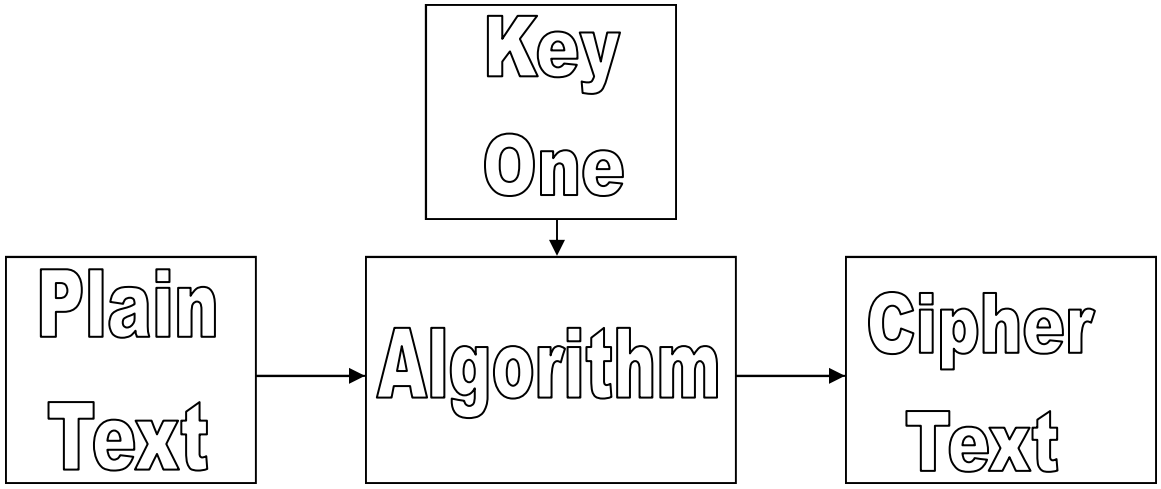
- Confidentiality -- Encryption
  - Only authorized people –e.g., the sender and recipient of a message, not eavesdroppers – can know the message.
- Integrity – Message Digests (MAC or MIC), and Digital Signatures
  - When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- Authentication – PKI and Digital Signatures
  - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- Nonrepudiation – MAC and Digital Signatures
  - Alice cannot later deny that the message was sent.
  - Bob cannot later deny that the message was received.

  - *Note: cryptography is not concerned with availability.*

Confidentiality/Encryption Goal

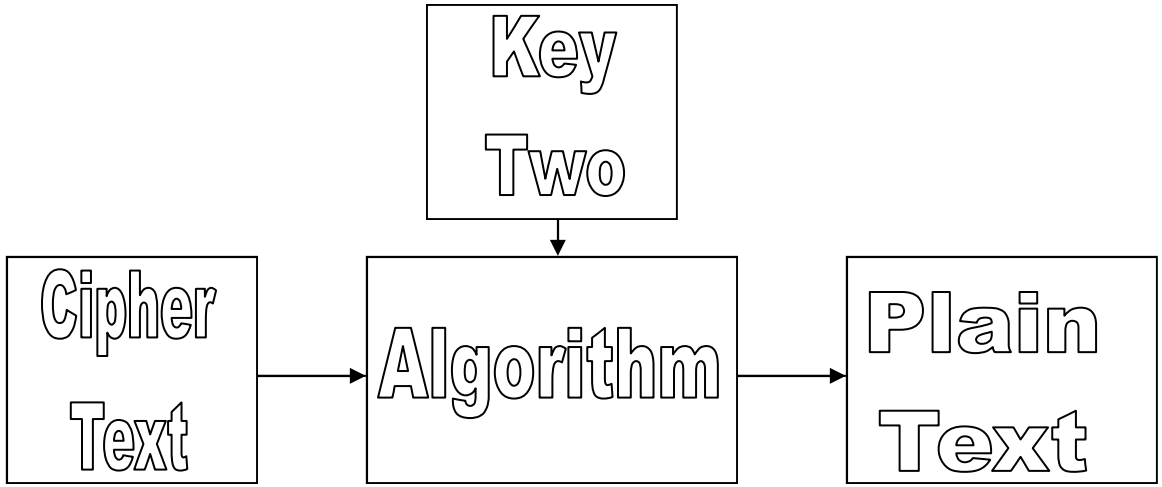
- Make obtaining or altering information too expensive, in time or money, to be worthwhile.
- Encryption strength is context sensitive.
  - Related to time as well as to the information's perceived value to the opponent.
- Cryptography doesn't need to be perfect, it just has to be stronger than your opponent's methods and resources.
  - Jay's rule – A cryptographic implementation should cost less than bribing the clerk that holds the information.

Encryption Process



- Key One and plain text are inputs into the encryption algorithm.
- Cipher text is the output.
  - In contrast to plain text, cipher text maintains confidentiality when sent through an insecure communications channel.

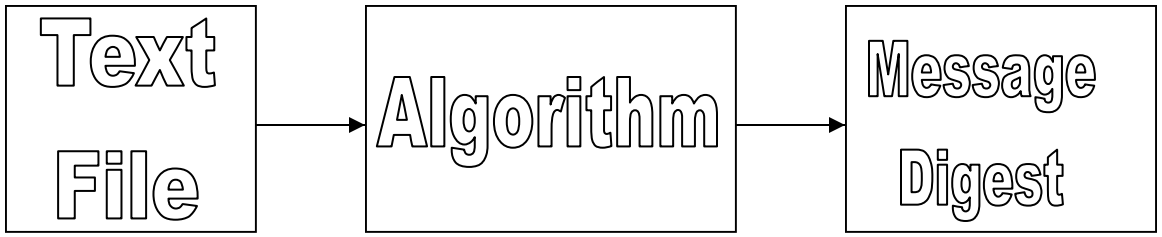
Decryption Process



- Key Two and cipher text are inputs into the decryption algorithm. Plain test is the output.
  - When using a symmetric algorithm, Key One and Key Two are identical.
  - When using an asymmetric algorithm, Key One and Key Two are different.

    Asymmetric notes
    - For confidentiality, sender uses the recipient's public key.
    - Then, since the recipient, is the only person with the private key, the recipient is the only person that can decrypt the cipher text.

An Integrity Process



- A Hash, or message digest, enables you to discern whether or not a document has been altered.
  - That is, it proves or disproves data integrity.
  - This process is also called a Message Integrity Code (MIC)
  - A hash is considered bound to a document.
    - Sometimes called a digital fingerprint.
- Process utilizes a one way function, called a hash.
  - Hash process takes a variable length document as input and produces a fixed length document as output.
- Hashes can also be components of digital signatures and Message Authentication Codes (MACs).
- This is an example of a keyless hash process.
  - Later, we will cover keyed integrity processes called message authentication codes (MACs or HashMACs).

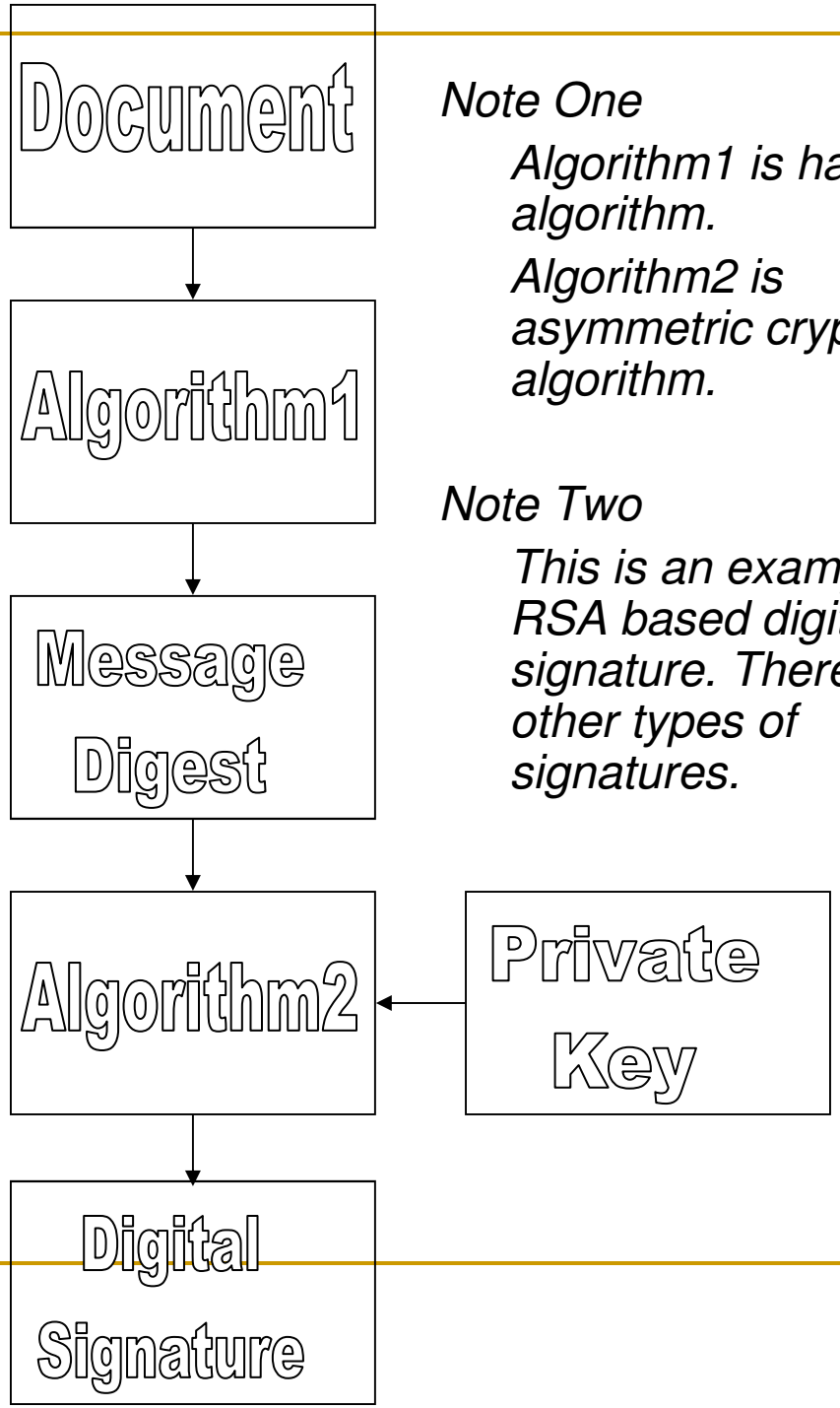
Authentication and NonRepudiation Goals and Process

- Authentication verifies that a message came from whom it is represented to come from.
- Non repudiation provides evidence so that a message can not be disavowed at a later time.

- Process utilizes a secret known to only one person (private key).
- Methods include digital signatures.

RSA Digital Signature Creation

1. Hash document to create digest
2. Encrypt hash with senders private key
3. Attach to encrypted hash communication
4. Upon delivery, recipient decrypts hash with senders public key
5. Creates new document hash and compares
6. If hashes are identical, documents have integrity.



Note One

Algorithm1 is hash algorithm.

Algorithm2 is asymmetric crypto algorithm.

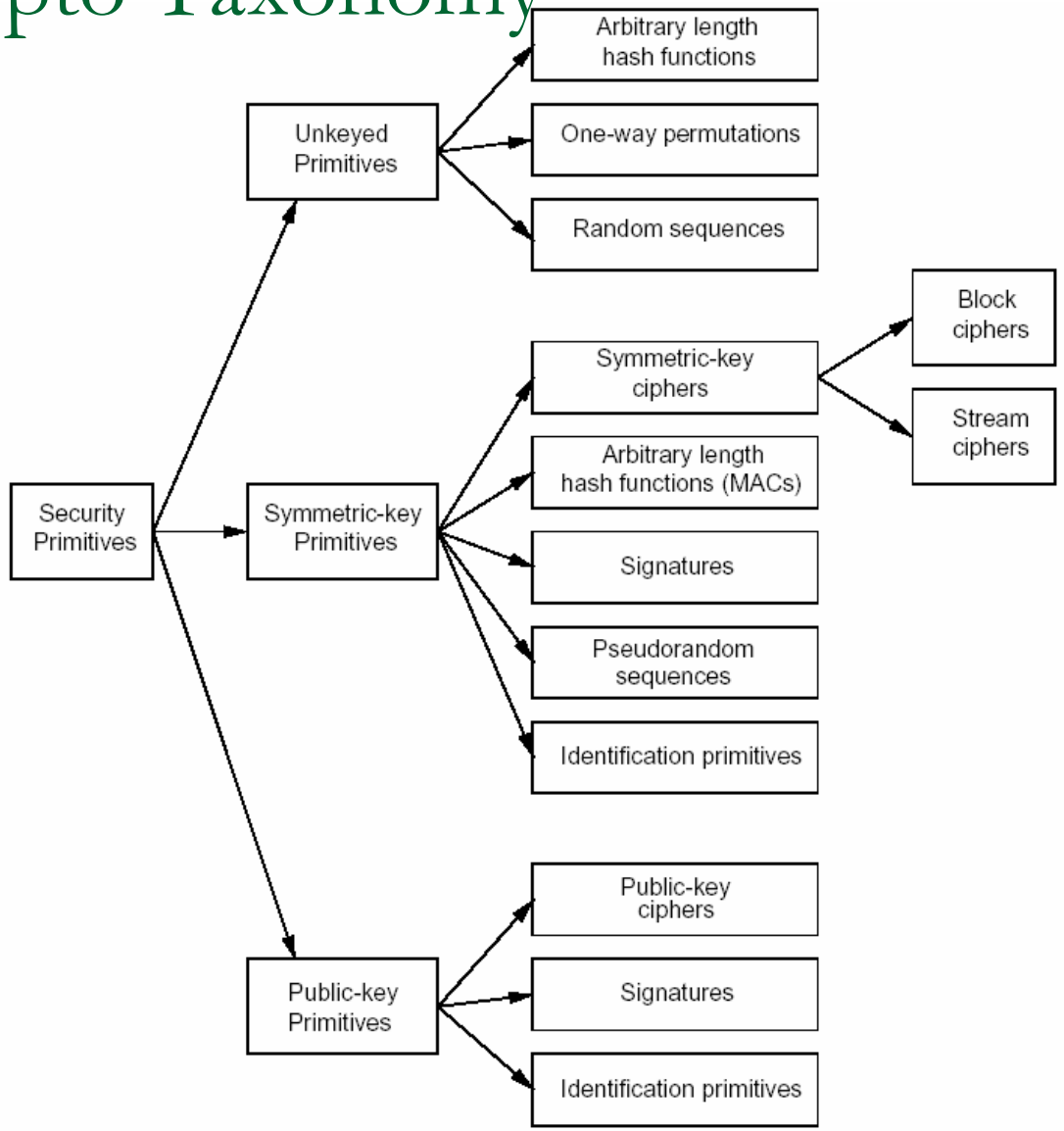
Note Two

This is an example of an RSA based digital signature. There are other types of signatures.

Cryptography Evolution

- Ciphers Done by Hand
  - Monoalphabetic
  - Polyalphabetic – Vigenere Cipher
  - Utilize transposition and substitution aka confusion and diffusion
- Ciphers Done by Machine
  - Engima
  - Purple
  - Sigbus
- Ciphers Done by Digital Computers
  - Symmetric
  - Asymmetric
  - Hybrid Cryptosystems
- Quantum Computer Future?

Sample Crypto Taxonomy



Modern Ciphers

- Historically, the substitution and transposition utilized by both monoalphabetical and poly-alphabetical ciphers proved vulnerable to frequency analysis attacks.
  - For several hundred years, polyalphabetic ciphers were considered unbreakable.
    - Babbage and Kasiki proved otherwise.
- Consequently, most modern ciphers use long sequences of complicated substitutions and permutations.

One Cipher to Rule them All!

One Time Pad

- A special implementation of the Vernam Cipher where:
  - Identical key and message lengths.
  - Key must be totally random.
  - Each key must only be used one time for only one message.
  - Key must be securely distributed
- If done properly creates an unbreakable cryptosystem.
  - Only cipher mathematically provable unbreakable.
- Impossible to do a real world implementation.
- Considered impractical. For more info see NSA's Venona project.

http://www.pro-technix.com/information/crypto/crypto_frame.html

Questions?

Selected References One:

http://cis.gsu.edu/~rbaskerv/cis8680/Lessons/crypto/index.html

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/

http://www-106.ibm.com/developerworks/library/s-pads.html

http://www.math.temple.edu/~renault/cryptology/affine.html

Selected References Two

https://www.isc2.org/cgi-bin/request_studyguide_form.cgi?AG=6042

http://www.microsoft.com/resources/documentation/windows/2000/server/reskit/en-us/distsys/part2/dsgch14.mspx

http://www.fas.org/irp/nsa/rainbow.htm

Appendix

- Who am I?

Who am I?

- Developed four, three credit hour, graduate level UH Security Courses
- Past Security Presentations at: University of Indiana in Pennsylvania's Network Security Workshop, Infragard, ISACA, ACM SIGITE, and American Association for Engineering Education
- Created/presented workshops at the New Jersey Institute of Technology and Sam Houston State University.
- Earned CISSP, NSA IAM & IEM, Security Certifications
  - Usual certifications from usual suspects (Cisco, CompTIA, Novell, and Microsoft).
- Former Network Admin and IS Director
- Graduate Military Police Academy
  - USARPAC German Shepard Sentry Dog School
  - Secret Clearance (expired)