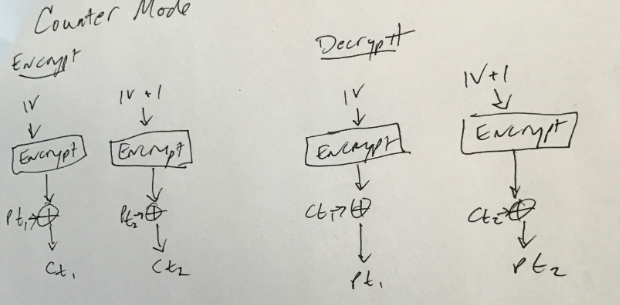
**MSDS 7349 Data and Network Security**

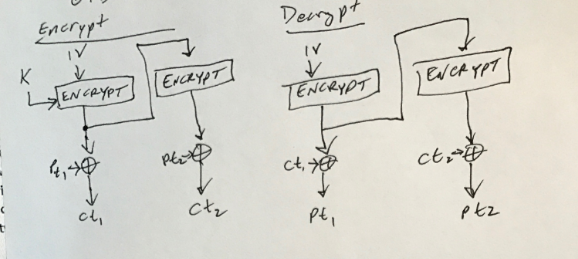
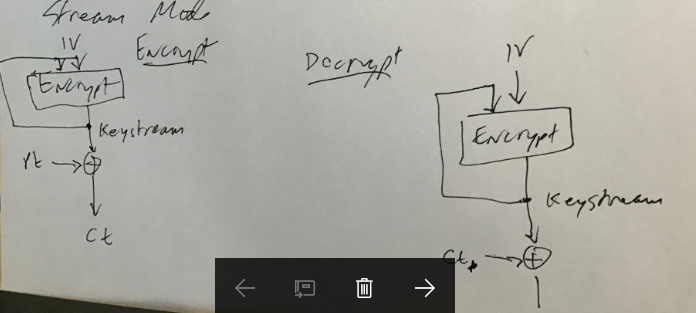
**Exam 1**

Name: Andrew Abbott

Date: 3/13/2017

1. 1. An encrypted message. An encrypted message is known as ciphertext.
   2. An algorithm for performing encryption and decryption. The process of converting plaintext to ciphertext and restoring from the ciphertext is known as a cryptographic system or a cipher. Textbook ch. 3.
   3. A zero. May refer to a type of proof or a part of key generation.
   4. A code. A code may be part of a cipher but a cipher is the system/algorithm.
2. 1. Counter Mode: Counter mode encrypts the IV and XORs the output with the Pt. The next block the IV is incremented before encryption. It turns a block cipher into a stream cipher. The stream is derived from incrementing the IV.



* 1. Output Feedback Mode: In OFB, a key is used to encrypt an initialization vector (IV). This output is XORed with the plaintext for encryption and also used as the IV for the next block. 
  2. Stream Mode: Here a keystream is created from the encrypted IV, it is XORed with the Pt and also encrypted again for each block. Often used as a synonym for OFB mode.
  3. All of the above.: Since OFB mode and Stream mode are often used as synonyms and counter mode also acts as a stream, all are correct.
  4. None of the above.

1. 1. Cryptography Encryption and Decryption: Cryptographic encryption and decryption relies on trusting key holders to keep secrets.
   2. Trust: This is the foundation of all security online.
   3. Authentication: This relies on some method such as Hashing, which must be trusted.
   4. Public Key Certificates: PK certificates must be managed by a trusted third party.
   5. Digital Signatures: These also must be maintained by a trusted third party.
2. 1. Security means the coercive capability to stop an aggressor. Security is freedom from war, and the ability to deter or defeat aggressive attacks.
   2. Security refers to safety from vulnerabilities (both external and internal) that could harm the state, societies within the state, and the values of those societies.
   3. Security means freedom to enjoy the things that are most important to human survival and well-being, such as food, health care, and the opportunity to live well.
   4. All of the above. – These answers describe national security and personal security. They do not mention network or cyber security. According to the Stallings textbook, computer security is “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.”
   5. None of the above.
3. 1. Counter Mode: Because each block does not depend on a prior block for its encryption, counter mode can be decrypted in parallel. Each block’s IV is just the original IV plus a number.
   2. Cypher Block Chaining Mode cannot be decrypted in parallel because it acts as a chain. Each block’s input into the encryption algorithm is the XOR of the current Pt and the previous block’s Ct.
   3. Electronic Codebook Mode: ECB cannot be decrypted in parallel because decryption is performed one block at a time with the same key.
   4. All of the above.
   5. None of the above.
4. 1. The hash value is preimage resistant: For any given hash value h, it is computationally infeasible to find y such that H(y) = h. It should be virtually impossible to generate the message from the code.
   2. The hash value is second preimage resistant: For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x). This prevents forgery or alteration of a message.
   3. The hash values are collision resistant. It is computationally infeasible to find any pair (x, y) with x ≠ y, such that H(x) = H(y). It should be impossible to find 2 messages that generate the same hash value.
   4. All of the above. The above descriptions are from the textbook, Ch. 11.
   5. None of the above.
5. 1. Hacker: The definition of hacker according to Merriam-Webster includes “a person who illegally gains access to and sometimes tampers with information in a computer system.”
   2. Identity Thief: Identity theft does not necessarily involve computers, stealing identification papers and pretending to be someone else is a form of ID theft and does not involve access to a computer.
   3. Intruder: Likewise, an intruder is someone who unwantedly gains access to a location, whether a computer system or a physical location. A hacker is an intruder, but not all intruders are hackers.
   4. Cyber-terrorist: Cyber-terrorists are often a subset of hackers who seek to cause harm with a goal in mind. This is much more than just gaining access illegally.
6. 1. E-mail privacy: Email privacy is an ethical issue because it involves potentially private information or secrets not intended for the public. Emails can contain anything from trade secrets to national security secrets. The protection of email privacy is important.
   2. Software piracy: This is also an ethical issue because it is easy to obtain copies of software without purchasing it. The creators of that software rely on that revenue for their livelihood and the ability to create more software.
   3. Intellectual property rights and copyrights: Like software piracy, IP is easily and often copied and resold or rebranded. The credit and income should go to the creator of the idea.
   4. All of the above.
   5. None of the above.
7. 1. Scalability: This is desired. Any test on a sequence can be applied to a random subsequence as well.
   2. Backward predictability. It should not be feasible to determine the seed from knowledge of any generated value.
   3. A shared initialization vector: If you have a shared seed someone could figure out the algorithm. Seeds should be random and unpredictable.
   4. All of the above.
   5. None of the above.
8. 1. Hash function: The main use of hash functions is data integrity. Any change to an input would change the output.
   2. Private key operation: Use of a private key can provide both authentication and integrity. Because only the sender could have used the private key, it authenticates the source. Since the message cannot be altered without the private key it also provides integrity. Its primary use is not just for integrity.
   3. Symmetric key operation: Like private key operation, the primary use of symmetric key operation is not to provide integrity protection but authentication and privacy.
   4. All of the above.
   5. None of the above.
   6. Shared Secret Key: Introducing a shared secret key actually changes the nature of the cipher. It would be a different cipher.
   7. Keep Algorithm Details Secret: Keeping the algorithm details secret does improve the strength of a cipher. It makes cryptoanalysis more difficult through confusion.
   8. Use a Key with a Larger Number of Bits: Increasing the length of the key does improve security, but it would be a different cipher as a result.
   9. All of the above.
   10. None of the above.
9. 1. Use both linear and non-linear functions.: The more non-linear, the better.
   2. Use one or two more rounds than the minimum to achieve randomness.: The number of rounds is chosen so that cyptanalytic efforts require more effort than a brute force attack.
   3. Have good avalanche properties.: Avalanche property means any change in the plain text will produce a larger change in the ciphertext. This is a basic design principle/
   4. All of the above.
   5. None of the above.

Source: Chapter 4, section 5.

1. 1. Grain 128-A: Does include authentication.

Ågren, Martin, et al. "A new version of grain-128 with authentication." *Symmetric Key Encryption Workshop*. Vol. 2011. 2011.

* 1. Hummingbird 2: Is also an authenticated encryption algorithm. I’ve heard great things about this author.

Engels, Daniel, et al. "The Hummingbird-2 lightweight authenticated encryption algorithm." *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Springer Berlin Heidelberg, 2011.

* 1. Keyak: This is also an authenticated cipher.

Wetzels, Jos, and Wouter Bokslag. "Sponges and Engines: An introduction to Keccak and Keyak." *arXiv preprint arXiv:1510.02856* (2015).

* 1. All of the above.
  2. None of the above.
  3. The public key encrypts only, so it must take the plaintext as input.: Either of the two related keys can be used for encryption, with the other used for decryption. Therefore it may take the ciphertext as input when used for decryption.
  4. The private key is used only for decryption of ciphertext encrypted with the public key.: Either of the two related keys can be used for encryption, with the other used for decryption.
  5. In RSA theory, once keys are calculated, if the ‘public key’ is kept secret and the ‘private key’ is made public, the cipher is not secure.: In this case the cipher is still secure. The labels ‘public key’ and ‘private key’ and ‘private key’ are reversed.
  6. All of the above.
  7. None of the above.

1. 1. Message authentication code modification: Modifying the MAC for reasons such as masquerade or message modification. A secure MAC would not be secure of it did not counter modification.
   2. Message modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification. Secure message authentication codes help to ensure the message is authentic and has not been modified.
   3. Source repudiation: Denial of transmission of message by source. A secure MAC acts as a digital signature and can counter source repudiation attacks.
   4. All of the above.
   5. None of the above.
2. The birthday paradox refers to the unintuitive probability that in a group of people there is a pair that share the same birthday. For instance, in a group of n people, there are (n\*(n-1))/2 pairs, for n=10, 45 pairs. The probability that any particular pair shares a birthday is 1/365 = 0.27%, but the probability that at least one pair shares a birthday is 88.4%. It would take about 8 groups of 10 to get a 50% chance of finding a matching pair.

In the security context, the birthday paradox refers to the ability of an adversary to create a collision, or create a second method with the same hash as a first. Given a hash of a particular bit size, the amount of time and processing required to brute force attack is less than expected. For example, a 16 bit hash has a 50% probability of collision after only 301 attempts. Given the processing power of today’s computers the size of a hash becomes very important for security.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **The birthday paradox** | | |  |  |  |  |  |  |  |  |
|  |  | **Probability of Random Collision** | | | | | | | | |
| **bit size** | **Possible outputs** | **1E-15** | **1E-12** | **1E-09** | **1E-06** | **0.1%** | **1.0%** | **25.0%** | **50.0%** | **75.0%** |
| 16 | 65536 | 0.00001 | 0.0004 | 0.01 | 0.4 | 11 | 36 | 194 | 301 | 426 |
| 32 | 4.3E+09 | 0.003 | 0.1 | 3 | 93 | 2932 | 9291 | 49711 | 77163 | 109125 |
| 64 | 1.8E+19 | 1.9E+02 | 6.1E+03 | 1.9E+05 | 6.1E+06 | 1.9E+08 | 6.1E+08 | 3.3E+09 | 5.1E+09 | 7.2E+09 |
| 128 | 3.4E+38 | 8.2E+11 | 2.6E+13 | 8.2E+14 | 2.6E+16 | 8.3E+17 | 2.6E+18 | 1.4E+19 | 2.2E+19 | 3.1E+19 |
| 256 | 1.2E+77 | 1.5E+31 | 4.8E+32 | 1.5E+34 | 4.8E+35 | 1.5E+37 | 4.8E+37 | 2.6E+38 | 4.0E+38 | 5.7E+38 |
| 512 | 1.3E+154 | 5.2E+69 | 1.6E+71 | 5.2E+72 | 1.6E+74 | 5.2E+75 | 1.6E+76 | 8.8E+76 | 1.4E+77 | 1.9E+77 |
| **Table shows the number of variables of each bit size needed to achieve the given probability of a random collision.** | | | | | | | | | | |
|  | | | | | | | | | | |

1. * 1. Application Layer: **S/MIME** provides a secure and consistent way to send and receive MIME (multipurpose internet mail extension) data. Per RFC 5751, “Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size.” S/MIME data is received or sent by software that does the interpretation or creation of the content.

S/MIME currently uses SHA-256 for digest and signatures but should be backward compatible with SHA-1 and MD5. It also uses RSA for key encryption. All or some of the capabilities may be used.

https://tools.ietf.org/html/rfc5751

* + 1. Transport Layer: **TLS** (Transport Layer Security) protocol “allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery”- RFC 5246. While applications use S/MIME to protect the content and authentication of content, TLS provides those applications with privacy and integrity as they communicate.

This protocol has two layers, the record protocol and the handshake protocol. The record protocol provides privacy and a reliable connection. The handshake protocol provides authentication, private sharing of secret keys, and a reliable negotiation.

<https://tools.ietf.org/html/rfc5246>

* + 1. Network Layer: **PPP OSI Network Layer Control Protocol** (OSINLCP) “provides a standard method of encapsulating Network Layer protocol information over point-to-point links” – RFC1377. The three parts of PPPOSINLCP are a method for encapsulating datagrams, a link control protocol, and a family of network control protocols.

The protocol establishes a point-to-point communication by sending LCP packets to set up and test the link, then NCP packets to set up the data encapsulating protocols.

https://tools.ietf.org/html/rfc1377

* + 1. Data Link layer: **PPP** (Point-to-Point) protocol standardizes the sending of datagrams over point-to-point links. It allows for access control, billing and other services to be handled at the user level rather than the site level. For PPP over Ethernet, the session learns the Ethernet address of the remote connection and establishes a unique session identification.

The two stages of PPP are the discovery stage and the session stage.

https://www.ietf.org/rfc/rfc2516.txt

* + 1. Physical Layer: **Ethernet** is the most common protocol used at the physical layer. This standard has many benefits including cost efficiency, scalability, protocol neutrality, ease of use, reliability and ubiquity.

Ethernet provides a set of physical media definitions, a scheme for sharing that media, and a addressing scheme for moving packets between devices.

<http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp001_-en-p.pdf>

1. 1. Buffer overflow attacks are the most common DoS attack. The idea is to overload the network system by sending more traffic than it can handle, then often to cause the system to execute the attacker’s code. One example of a buffer overflow attack is the 2001 Code red worm. The worm used a long string of the letter ‘N’ to overflow a buffer in computers running Microsoft’s IIS web server. Source: <https://en.wikipedia.org/wiki/Code_Red_(computer_worm)>

One method of defending against these types of attacks is to write correct code in the first place. Another method is to make the buffer areas non-executable. Each of these methods and other methods have costs as well as benefits to be weighed.

*Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade\**

Cowan, et al.

<https://crypto.stanford.edu/cs155/papers/cowan-vulnerability.pdf>

* 1. DDoS (Distributed Denial of Service) is another type of DoS attack. This occurs when multiple or many systems conduct a simultaneous DoS attack on a target. This has the advantages of greater processing power, anonymity. An example of a DDoS attack is in 2012, the group Anonymous attacked supporters of the Stop Online Piracy Act (SOPA). They used a voluntary botnet.

The methods of mitigation involve monitoring traffic and cutting behaviors that could indicate an attack.

https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack

1. To defeat a man-in-the-middle attack during the process of establishing a secure connection, authentication must occur. An attack such as the one below, without authentication, allows Trudy to share a secret key with Alice and Bob and eavesdrop on their communication. To add authentication to this process, Alice first sends Bob her identity along with a nonce, encrypted using Bob’s public key. Trudy does not have Bob’s private key to decrypt the identity and nonce. Bob receives the message and decrypts it with his private key. He then answers with the original nonce and a new nonce encrypted using Alice’s public key. Alice receives the message and decrypts the second nonce. She then sends it back encrypted using Bob’s public key. Finally, Alice can send Bob the message encrypted using Bob’s public key and her own private key. This is shown in the second figure below. Any interception by Trudy is futile and Trudy trying to masquerade as Alice by sending her own public key with her own id would end in defeat as well.

