Cybersecurity Fundamentals

Contents

Crptography
- Definition of Cryptography
- Fundamental Terminologies
- Secret Writing branches
- Hash
- Symmetric and Asymmetric Encryption
- Use of Cryptool

Next

Definition of Cryptography

Cryptography definition

Cryptography is the art of private communication in a public environment

Notice: That definition does not contain the word "encryption".

Why?

Next

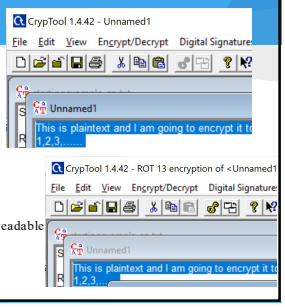
Fundamental terminologies

Terminologies

Plaintext/Ciphertext
- Plaintext =human readable
  - Also; Cleartext
- Ciphertext = non-human readable

Encryption
- Transform readable to nonreadable
- Also; Encipherment

Decryption
- Transform nonreadable back to original readable
- Also; Decipherment



Terminologies

Algorithm:

- The public knowledge set of rules behind cryptography
  - Modern cryptosystems utilize math for this
- Two modern Algorithms:
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - Thereare many others - these are the most common

Cryptanalysis:

- The art and science of breaking cryptography
- Also called Cryptanalytic Attack

Terminologies

Key: A numeric value of a given length (expressed in bits)

- The secret that must be protected
- The changing part ofthe algorithm that you must protect
- E.g. The Data Encryption Standard (DES) algorithm uses a 56-bit to create a Key

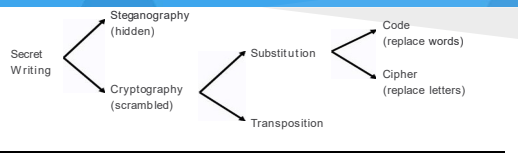
Keyspace: The range ofvalues that can be used to construct a key given a particular key length

- The total of all possible combination of l's and 0's given a specific number of binary bits
- E.g. DES uses a 56-bit to create a Key, total of all possible combination of l's and 0's (56 bits) is 72 followed by 15 zeros or 72,000,000,000,000,000 or 72 quadrillion = the size of the keyspace for DES

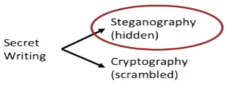
Next

Branches of secret writing

Secret Writing branches



Portions of this "tree" will appear as we move through the branches. For example:



Steganography: Hidden Cipher: Sir John Trevansion's Letter (1)

Worthie Sir John: Hope, that
much, I fear me, help you no
ever I may be able to requite
me: Tis not much I can do: bu
I knowe that, if deathe come

Hidden Cipher: Sir John Trevansion's Letter (2)

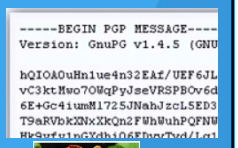
3rd Character after punctuation =

Worthie Sir John: Hope, th
cannot much, I fear me, h
is this only: if ever I may b
stand not upon asking me
do, bee you verie sure I w

Steganography vs. Encryption

Encryption (our next topic) provides:
- "Confidentiality of communication"
- NOT "Secrecy of communication"
- Nobody else knows what you are saying, but they can tell you are talking privately
- Humans and computers can spot cyphertext

Steganography provides:
- "Secrecy of communication"
- Nobody knows the parties are even talking
- Combined with crypto, you can get the best of both

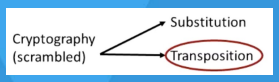


Just a pretty picture.

Encryption: Transposition/Permutation/Obfuscation (1)

Transposition ciphers is simply reordering the letters of a message:
- Think of a simple anagram-a rearranging of letters
- For example, take the word "cinema" and rearrange the letters to create "iceman":
  - In crypto, the new version of the letters are not always readable words ("cinema" into "emicna")

- You *transpose* the order of the letters
- You *permute* the order of the letters
- You *obfuscate* the order of the letters



Example (*Vigenere cipher*)

Key: d e c e p t i v e d e c e p t i v e d e c e p t i v e

Msg: w e a r e d i s c o v e r e d s a v e y o u r s e l f

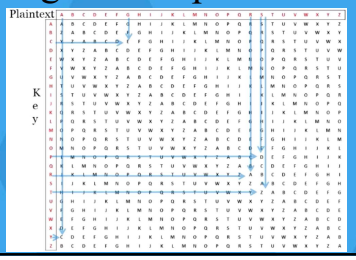
: z i c v t w q n g r z g v t w a v z h c q y g l m g j

Encrypt: key -> row and Msg -> column

Decrypt: key -> row the position of ciphertext letter determine the column, and plaintext letter is on top of that column

15

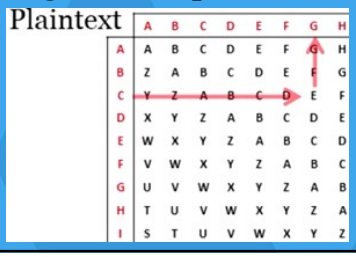
Vigenere Cipher Table (1)



GRASS = Plaintext

CRYPT = Key
EACDZ = Ciphertext

Vigenere Cipher Table (2)



EACDZ — Ciphertext
CRYPT = Key
GRASS = Plaintext

To decrypt: Take the first letter of the key (C).

Move down the left side to that letter.
Move over on that line to the first letter of ciphertext. In this example, it is the letter E, the seventh character over. The letter at the top of that line is the plaintext - G in this case.

Next

Hash functions

Message Digest: One-Way Hash

- Example:

At http://www.xoroin.com/tools/md5-hash-calculator
Paste the title "Message Digest: One-Way Hash" and click Calculate
The output is:
4df98231549beb91208800b53449d0f1

By changing the capital D to a lowercase d
The output is:
3297dc5d579bec4efa50ada046d3dc32
They are completely different (an Avalanche Effect)

If you hash all the text on the previous slide, the resulting hash is:

Adacdd931c512f0624056e34faf56c51

Still 128 bits, even though the input is significantly longer.

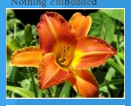
Message Digest: One-Way Hash

- Proper name = Message Digest: One-way hash is more common slang
  - Not encryption, but utilized by cryptosystems (Cryptosystems utilize hash functions)
  - Hashing software uses mathematical algorithm that runs against 1s and 0s of a file
  - The file is not modified in *any* way
  - Generates a fixed length hash from that file

- The hash is always the same length regardless of the file size:
  - That is, MD5 = 128-bit hash - SHA-1 = 160-bit hash - SHA-256 = 256-bit
- Provides no insight as to the input
- Must have a good Avalanche Effect

One-way Hash Example

Nothing embedded



With file embedded

```
$ md5 IMG_1132.JPG
MD5 (IMG_1132.JPG) = 8
```

Note: This tells us *that* the images are different but not *how* the images are different.

```
$ md5 embed_IMG_1132.JPG
MD5 (embed_IMG_1132.JPG)
```

Message Digest Version x: MDx

- The "MD Family" of hash algorithms created by Ron Rivest:
  - All generate 128-bit hash regardless of input size
  - All are public domain
- MD2:
  - Very slow
- MD4:
  - Much faster
- MD5:
  - Newer version of MD4
  - Much more complex, harder to break
  - Most common

- Secure Hash Algorithm (SHA, SHA-2, SHA-3): Group of hash algorithms

Secure Hash Algorithm: SHA

- SHA: Group of hash algorithms: Published by NIST
- SHA (or SHA-0) and SHA-1: Created 1993 to 1995:
  - Designed as part of the Digital Signature Standard (DSS), by US government
  - Generates a 160-bit hash
  - SHA-0 is considered flawed (was broken immediately) and no longer used
  - SHA-1 is extremely common today
- SHA-2 family:
  - Includes SHA2-224, SHA2-256, SHA2-384, and SHA2-512
  - Each produces a hash length described by its name (that is, SHA-256 produces a 256-bit hash) four different lengths of hashes available in this grouping.
- SHA-3 family chosen in 2012 as an eventual replacement:
  - SHA3-224, SHA3-256, SHA3-384, and SHA3-512 (same lengths as SHA2)
  - Based on different fundamental math (MD5, SHA-1, and all SHA-2 algorithms are based on the same fundamental math)

Symmetric vs Asymmetric

Symmetric-key encryption

25

Symmetric-Key Algorithms

- Advanced Encryption Standard: AES
- Data Encryption Standard DES and Triple DES

Symmetric Key Cryptography (1)

Commonly used for many years

The key that encrypts **must** decrypt:
- Vigenere cipher: Both sides require an identical key
- ROT13: Both sides rotate the alphabet by 13 positions

- Example of modern crypto algorithm

123 X ___ + 456

123 X Key 789 + 456

Cryptovariable

Must use the exact same key on each end of the communication
You have to protect the key and change it regularly

Symmetric Key Cryptography (2)

Disadvantage:

Difficult key management:
- Scalability: n*(n-1)/2
- Total number of keys required
- No nonrepudiation (digital signatures)

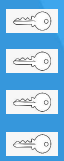
Advantage:
- Requires smaller keys to achieve same work factor as asymmetric:
  - In rough numbers: 128-bit symmetric = 3072-bit asymmetric
  - A 256-bit symmetric key = 15,360 prime # based asymmetric key
- Speed! 1,000 to 10,000 times faster than asymmetric

Asymmetric Cryptography (1)

- Two mathematically linked keys:
  - One called the "Public Key"- One called the "Private Key"
    - Give the public key to anyone-Keep the private key to yourself (passphrase protected)
  - Possession of one key does not allow you to discern the other key
  - The key that encrypts **cannot** decrypt:
    - Just backward of symmetric-and the most fundamental difference
  - Anything encrypted by one key can ONLY be decrypted by the mathematically linked key
- Allows for four processes:
  - Encrypt to send
  - Decrypt to read
  - Create digital signature
  - Verify digital signature

Asymmetric Cryptography (2)

	Four Processes
1	Encrypt to send
2	Decrypt to Read
3	Create Signature
4	Verify Signature



You have to use the correct key with each of those processes

How can you figure this out?
- Ask a series of questions and answer them logically
- Do it correctly, it will bring you to the correct key

Asymmetric Cryptography (2)

	Four Processes	Who is doing it?	Which keys do they have?	What is the goal?	Which Key I use?
1	Encrypt to send	Sender	• Sender Private • Sender Public • Recipient Public	Only Recipient can read	Key associated with Recipient -- Recipient Public -

- **Answer these questions logically and you will always get the correct answers.**
- **Answer these questions correctly and you will always arrive at the correct key.**

Asymmetric Cryptography (2)

	Four Processes	Who is doing it?	Which keys do they have?	What is the goal?	Which Key I use?
1	Encrypt to send	Sender	• Sender Private • Sender Public • Recipient Public	Only Recipient can read	Key associated with Recipient -- Recipient Public -
2	Decrypt to Read	Recipient	• Recipient Private • Recipient Public • Sender Public	Only Recipient can read	Key only Recipient has -- Recipient Private --

- **Answer these questions logically and you will always get the correct answers.**
- **Answer these questions correctly and you will always arrive at the correct key.**

Asymmetric Cryptography (2)

	Four Processes	Who is doing it?	Which keys do they have?	What is the goal?	Which Key I use?
1	Encrypt to send	Sender	• Sender Private • Sender Public • Recipient Public	Only Recipient can read	Key associated with Recipient -- Recipient Public -
2	Decrypt to Read	Recipient	• Recipient Private • Recipient Public • Sender Public	Only Recipient can read	Key only Recipien t has -- Recipient Private --
3	Create Signature	Sender	• Sender Private • Sender Public • Recipient Public	Prove it came from Sende r	Key only Send er has -- Sender Private --

- **Answer these questions logically and you will always get the correct answers.**
- **Answer these questions correctly and you will always arrive at the correct key.**

Asymmetric Cryptography (2)

	Four Processes	Who is doing it?	Which keys do they have?	What is the goal?	Which Key I use?
1	Encrypt to send	Sender	• Sender Private • Sender Public • Recipient Public	Only Recipient can read	Key associated with Recipient -- Recipient Public --
2	Decrypt to Read	Recipient	• Recipient Private • Recipient Public • Sender Public	Only Recipient can read	Key only Recipien t has -- Recipient Private --
3	Create Signature	Sender	• Sender Private • Sender Public • Recipient Public	Prove it came from Sende	Key only Sende r has -- Sender Private --

Asymmetric Cryptography (3)

- Before using this type of crypto, there MUST be a key exchange:
  - If Alice and Bob are going to talk, then …
  - Alice must give Bob her public key
  - Bob must give Alice his public key:
    - How they accomplish this does not matter
    - Anybody can have Alice's and Bob'spublic key
    - So, a secure distribution channel is not necessary
  - Alice needs her private key and Bob's public key
  - Bob needs his private key and Alice's public key

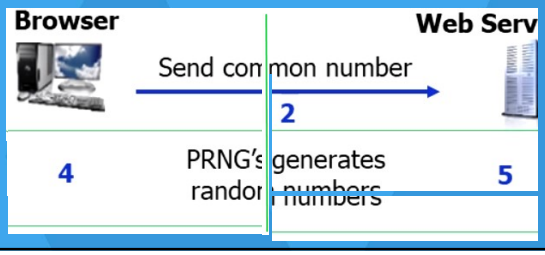
Asymmetric Cryptography Algorithms

- Diffie-Hellman
- Asymmetric Key: RSA
- The Elliptical Curve Cryptosystem ECC

Asymmetric Key: Diffie-Hellman

- 1976: The first asymmetric algorithm
- Perhaps the most used, unknown protocol:
  - IPSec, SSH, SSL, TLS, and others
- Has one purpose:
  - Two computers that may never have communicated before can securely exchange a symmetric key for data encryption
- Is public domain
- Based on prime numbers

How Diffie-Hellman Works (1)



How Diffie- Hellman Works (2)

How can this be secure if the common number (2) and the calculated numbers (16 & 32) are passed in the clear???

- The attacker would have to predict the PRNG generated numbers (4&5 in the example)
- In the last slide, we used 2, 4, and 5, but those are actually 4,096-bit numbers
- Which are 1,234-digit decimal values
- So the example numbers of 2, 4, and 5 we used really look like this:

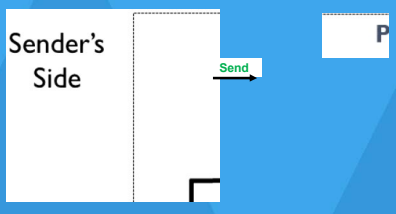
Symmetric and Asymmetric Compared

Symmetric Key that encrypts must decrypt	Asymmetric Key that encrypts cannot decrypt
➢Not based on prime numbers • Meaning it is much faster • Smaller key size in brute force	➢ Based on prime numbers* • Much slower • Much larger key required
➢Difficult key management • Protection of the key is paramount • Any compromise of key = compromise of data encrypted by that key	➢ Easy key management • So long as you protect private key (encrypted by a passphrase) • Share public keys with everyone you want to talk to

Digital Signature (1)

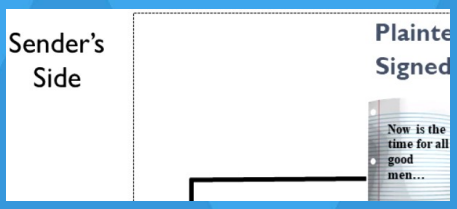
- A generic term to describe a process to:
  1. Verify who sent the document
  2. Verify the document received is the exact same document that was sent
- The detailed steps to generate and verify a signature vary with different implementations
- An example follows

Digital Signature (2)



They are aiming only to attain integrity.
They want to prove that:
1. Alice sent the message
2. message Bob receives is the same as the one Alice sends

Digital Signature (2)



1. Because Alice's public key was able to decrypt the signature, it authenticates to Bob that only Alice could have sent the message.
2. Because the hash from the signature and the new hash match in step 7, the message Bob received, and the message Alice se are exactly identical. In fact, every binary bit is the same.

Digital Signature and Nonrepudiation

- A proper digital signature results in nonrepudiation:
  - The sender cannot repudiate or deny having sent the document
  - This can stand up in court, just as a pen-and-ink signature can
- To prove nonrepudiation, the receiver must prove **two** facts:
  1. The person he thinks sent the document did in fact send it
  2. He received exactly the same document the sender sent
- If the sender's public key can decrypt the signature, this authenticates that it came from the sender:
  - See Certificate Authority discussion later for how to obtain proof
- If the hash in the signature and the hash generated by the receiver match, then what was received is what was sent
- Properly completed digital signatures may be legally recognized in 68 countries

Hybrid Cryptography

- Digital signatures provide for **nonrepudiation** and **integrity**. They do **not** provide for **confidentiality**

Hybrid Cryptography:

- Implement both symmetric and asymmetric cryptography at the same time
- Extremely common cryptographic process
- Proper implementation gives you:
  - The speed of symmetric key
  - Ease of use of asymmetric key
  - Security of sending ciphertext
  - Protection of the symmetric key in transmission

Signcryption

- Hybrid cryptography is great:
  - But what if we want even more?
- How can we get the following all at once?
  - Nonrepudiation of a digital signature
  - Confidentiality of hybrid cryptography
  - Protection of the symmetric key
- We want it ALL!
  - And Signcryption is the answer

Signcryption Example Sender

Signcryption Example Sender

Signcryption Example Receiver

Signcryption Example Receiver

51

References

www.sans.org