Cybersecurity

Hashing and Digital Signatures

CYBER.ORG

What is Cryptography?

- Comes from the two Greek words *kryptos* and *graphein*
  - **Kryptos** meaning “a secret” or “to hide”
  - **Graphein** meaning “to study”
- Cryptography methods have been around for thousands of years
  - One of the first examples is a Caeser Cipher which would have been used in the early BC’s.

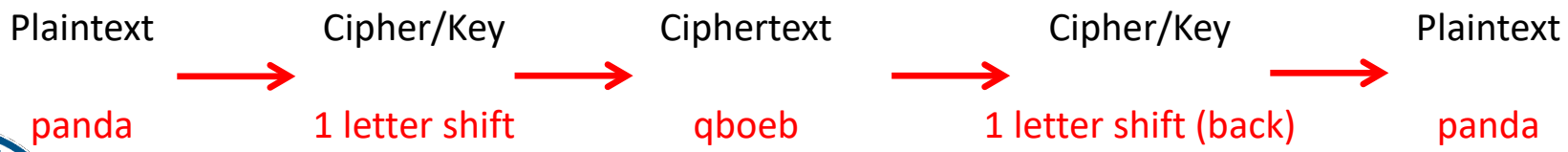
Example of a cipher disk used to help encode and decode a Ceaser Cipher

Cryptoanalysis

- The art (or study) of solving/cracking encryptions
- There are constantly people/research happening to find flaws and/or weaknesses in ciphers
  - No cipher is 100% secure, but how secure can we make them?

Cryptography Basics

- Plaintext
  - Message to be sent (not encrypted)
- Ciphertext
  - The message when encrypted
- Cipher (also known as a Key)
  - The algorithm that is used to encrypt and decrypt the message



Cryptographic Keys (Ciphers)

- Keep them private
  - You don’t want the public knowing how to decipher your messages
- The Key determines the output
  - Many different types of key
  - Some keys are one-way keys and cannot be undone
- Trust the process
  - Sometimes the algorithm is well known
  - However, the public does not know the individual key

Key Basics

- Do not use short keys
  - Helps prevent against brute force attacks
  - 128-bit or higher keys are common
  - A lot of keys use very high prime numbers
- How to exchange keys (across an unsecure medium)?
  - Key must remain a secret
  - Trusted domains help protect the keys
    - Diffie-Hellman is a common key exchange
  - Encrypt and protect the key exchange

Famous Ciphers

- Pigpen Cipher
  - Used by Freemason's in the 1700's
    - Letters represented by symbols

- Enigma Machine
  - Used by Germans in WWII
    - "Cracked" by some of the Allies

Hashes

- One-way algorithm
  - Encryption can only work one way, can not be reversed
  - Thus, you can not recover the original password
  - This helps keep password confidentiality
- Common uses
  - Verify a downloaded data is the same as the original data
- Digital signatures

Hash Examples

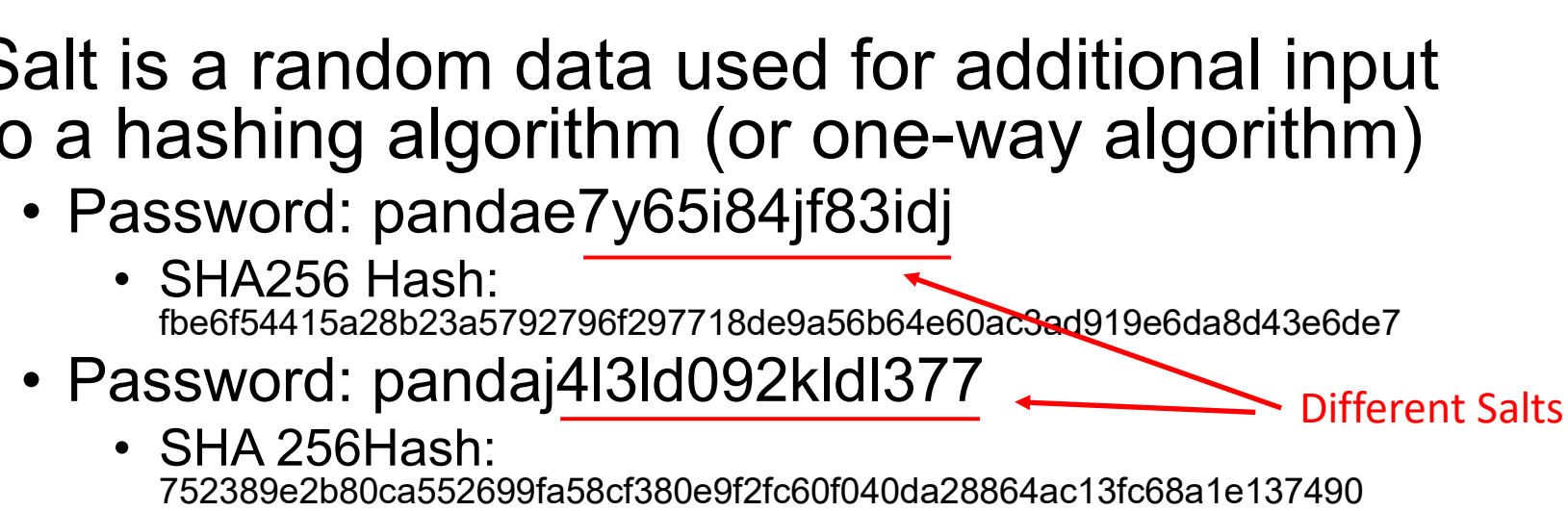
- SHA224 (224 bits)
  - Password: NICERC
    - SHA224 Hash: a771341621adb584d963401f83c50a727b8fd3268572830a50a42035
  - Password: nICERC
    - SHA224 Hash: 8f23d28facc5c604adb5f50196f60af70ec58d8e38d72deb3c461690
- MD5 (128 bits)
  - Password: NICERC
    - MD5 Hash: 962d07c231a9c3dd52822be8f857fb67
  - Password:NIcERC
    - MD5 Hash: ff12dfa035134708287d104b8e1acc0b

Collision

- Collision is two different inputs have the same output
  - Hashing should never have two different passwords have the same hash
    - Hash should be unique
- There are some examples where hashes give the same output
  - Very rare
  - 1 in a million if/when they are found

Salt, IV, Nonce

- Salt is a random data used for additional input to a hashing algorithm (or one-way algorithm)
  - Password: pandae7y65i84jf83idj
    - SHA256 Hash: fbe6f54415a28b23a5792796f297718de9a56b64e60ac3ad919e6da8d43e6de7
  - Password: pandaj4l3ld092kldl377
    - SHA 256Hash: 752389e2b80ca552699fa58cf380e9f2fc60f040da28864ac13fc68a1e137490
- IV (Initialization Vector) is mainly used in for wireless connections
- A nonce is a salt that is only used once



Practical hashing

	Username	PasswordHash
1	User1	e10adc3949ba59abbe56e057f20f883e
2	User2	5f4dcc3b5aa765d61d8327deb882cf99
3	User3	bf787577ff656cde5b5d1f8236a75d2a
4	User4	96e79218965eb72c92a549dd5a330112
5	User5	25d55ad283aa400af464c76d713c07ad
6	User6	d8578edf8458ce06fbc5bb76a58c5ca4
7	User7	25f9e794323b453885f5181f1b624d0b
8	User8	4297f44b13955235245b2497399d7a93
9	User9	22d7fe8c185003c98f97e5d6ced420c7
10	User10	0d107d09f5bbe40cade3de5c71e9e9b7
11	User11	827ccb0eea8a706c4c34a16891f84e7b
12	User12	81dc9bdb52d04dc20036dbd8313ed055

Stored Hashed passwords

- Storing Passwords
  - Hash is stored instead of actual password
  - Hashes will be compared instead of password
  - Original password can't be retrieved
- Verifying a downloadable file
  - Website provides the hash
  - If hash is the same, the document hasn't been altered
- Digital Signatures
  - Provides proof that a message was not changed
  - Also makes sure that a fake signature was not used
  - Contains both a private and public key

Signer signs document → Signature hashed (private key) → Document sent (Data and signature) → Data hashed (public key) → Signature hash and data hash are compared to verify