Course Summary

Stephen Haunts

@stephenhaunts | www.stephenhaunts.com

Security Requirements

Confidentiality

Security Requirements

Confidentiality

Integrity

Non-Repudiation

Authentication

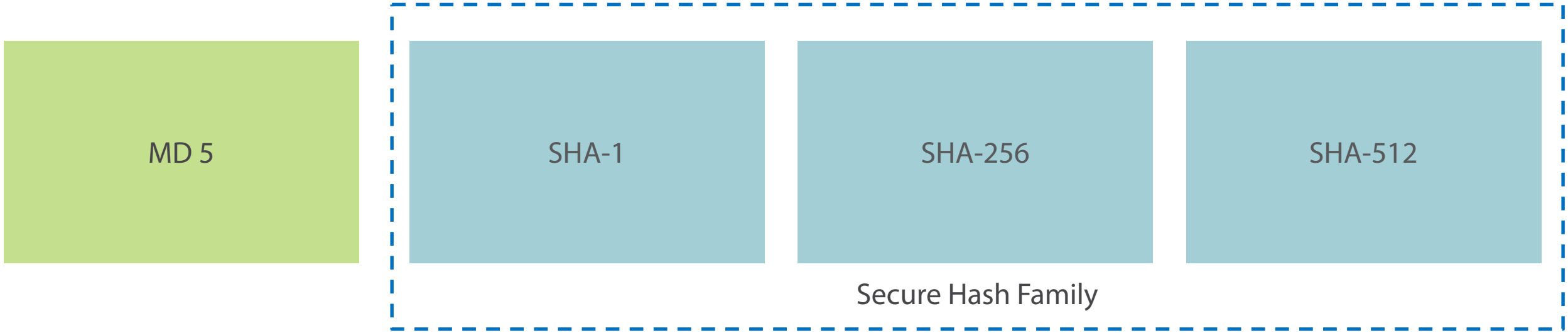
Random Numbers

- Random numbers are essential for generating encryption keys
- System.Random is not suitable
- Use RNGCryptoServiceProvider to generate random numbers
- RNGCryptoServiceProvider is much slower than System.Random

Hashing

- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash

Hashing



Hashed Message Authentication Codes

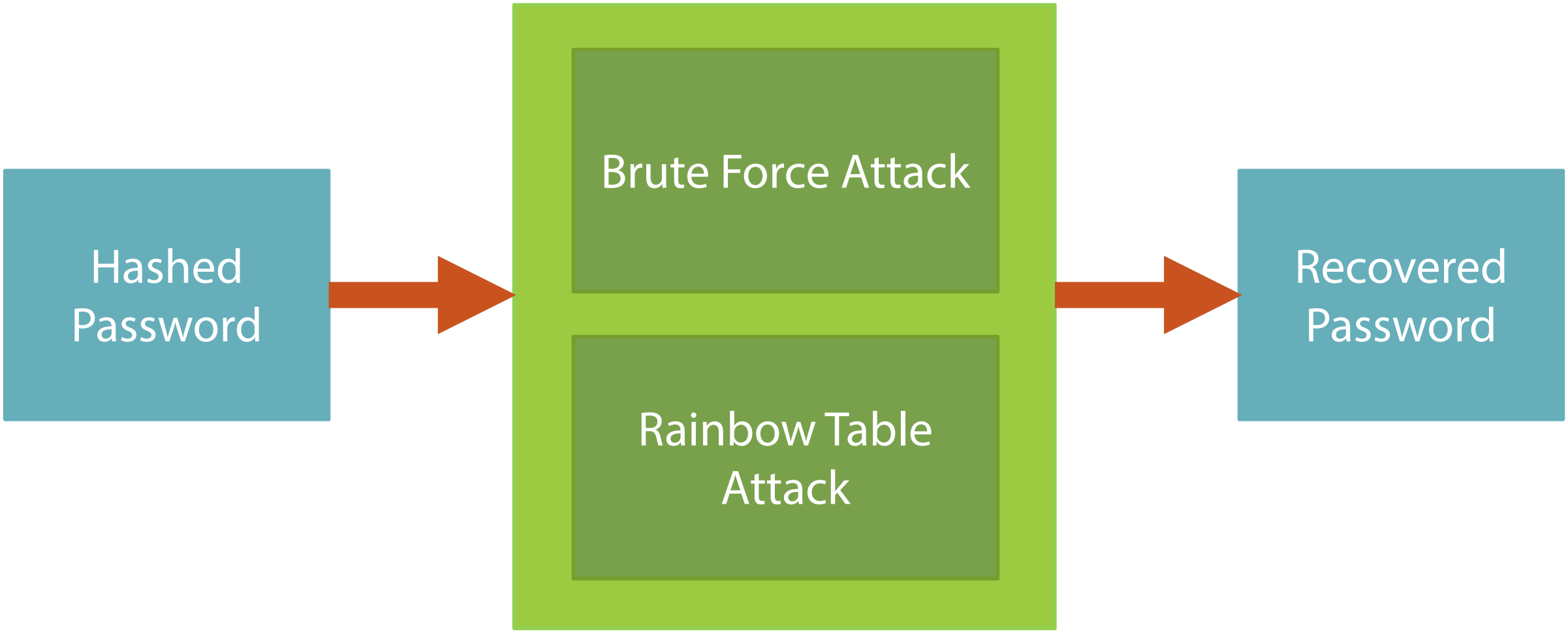
"This is a message we want to check the integrity of"

Hashed Message Authentication Code (HMAC)

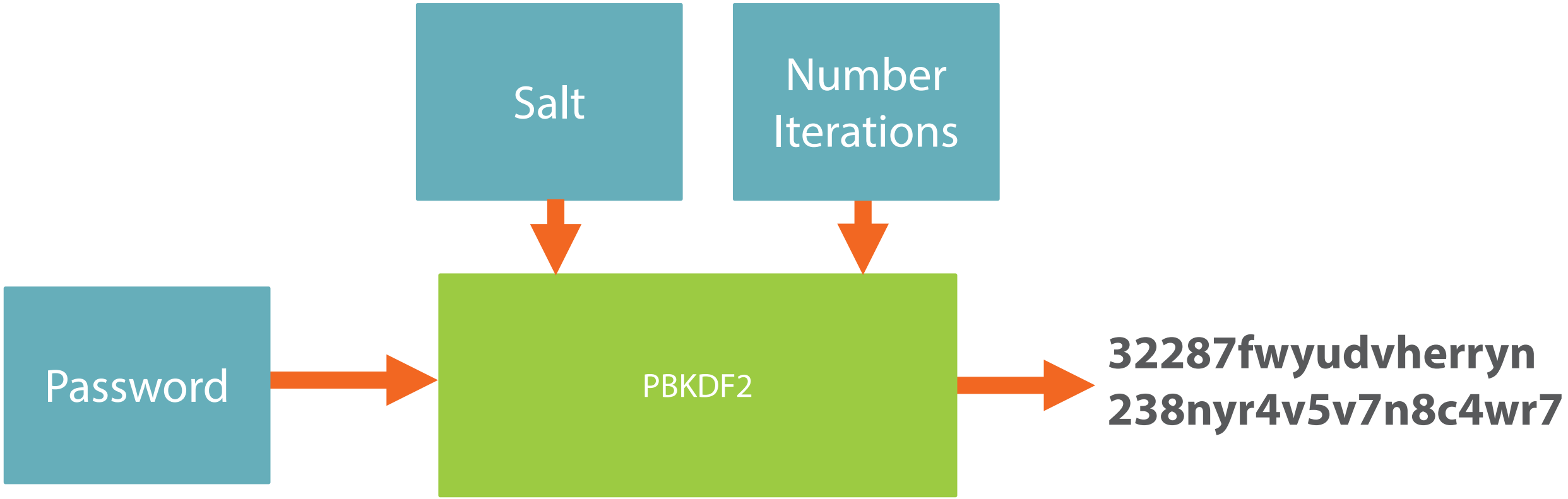
MD5 or SHA 1 and 2

87237yr87ny8t7wynt87eny588wenyrc8nwyvc8wnry8w7ny8wyr8cw7nyr8wn7e=

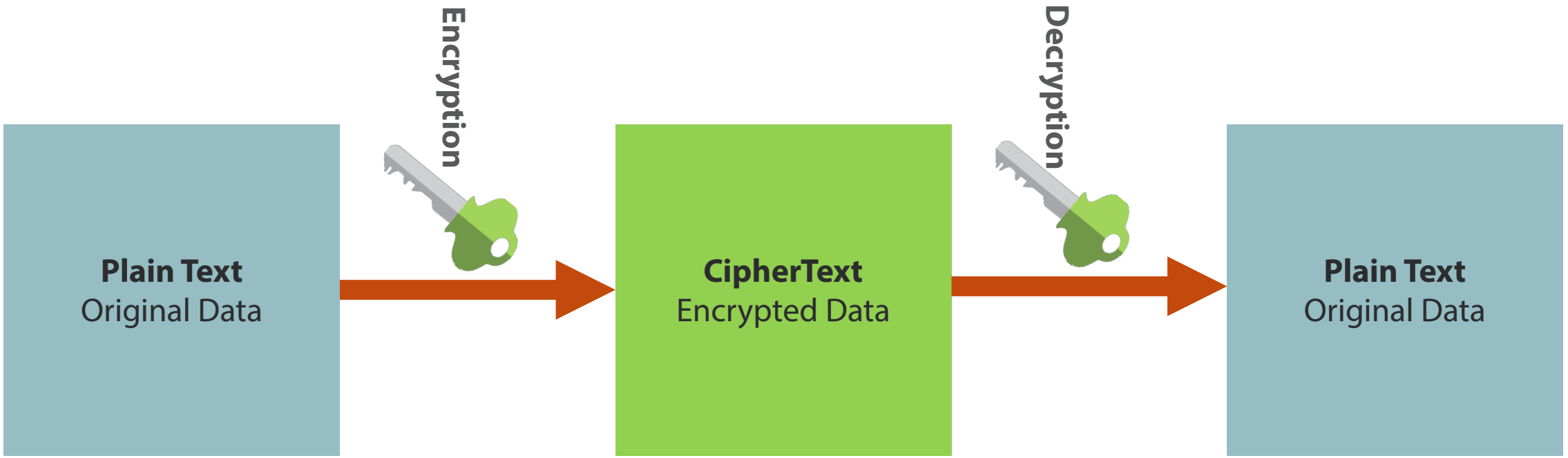
Storing Passwords



Password Based Key Derivation Functions



Symmetric Encryption



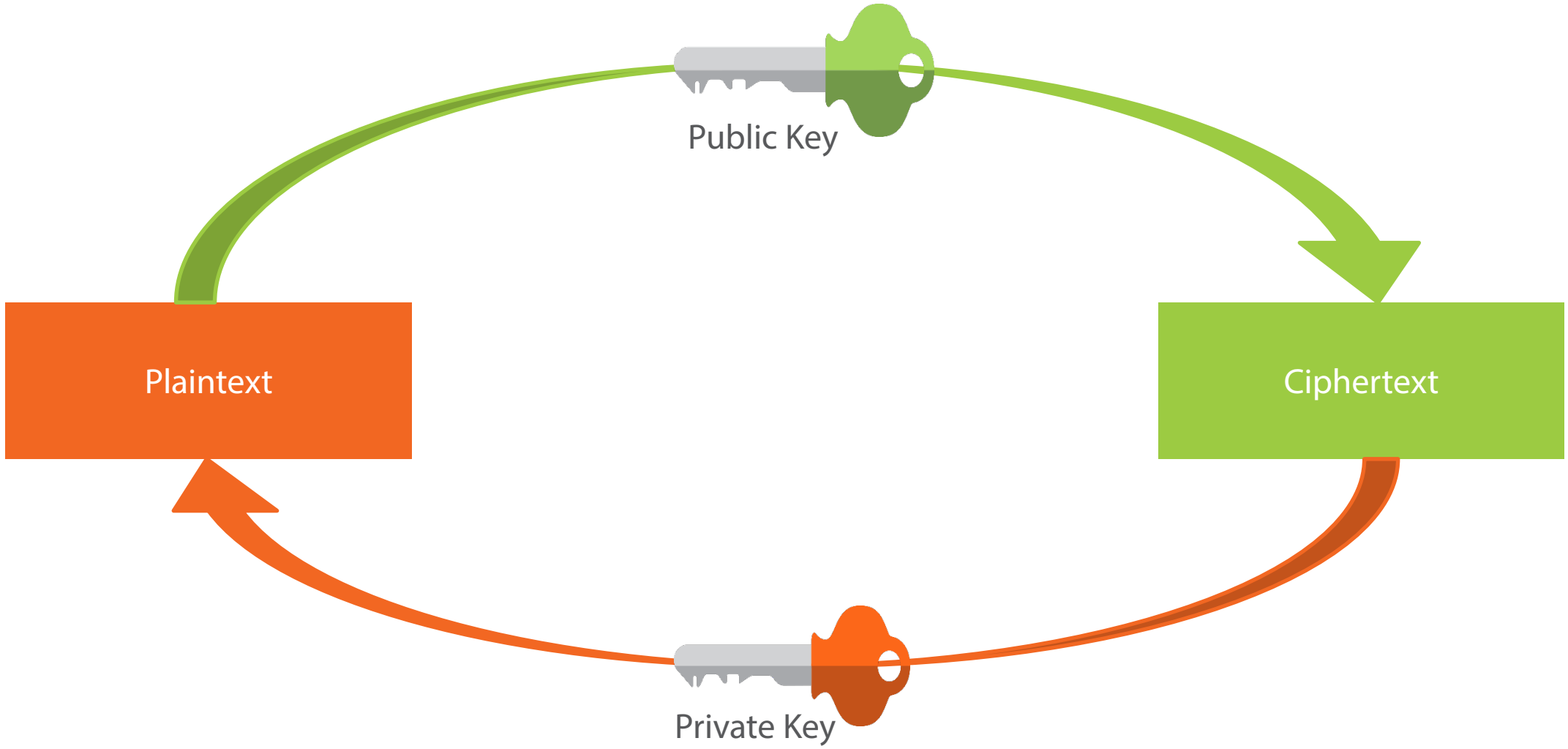
Symmetric Encryption

DES

Triple DES

AES

Asymmetric Encryption



Asymmetric Encryption

- RSA
  - 1024 bit keys
  - 2048 bit keys
  - 4096 bit keys

Hybrid Encryption

- Key sharing with symmetric encryption is hard to do securely
- Asymmetric encryption is a lot slower than symmetric encryption
- Asymmetric key sharing is a better solution
- Hybrid encryption combines the best of both worlds
- Symmetric keys are encrypted with asymmetric encryption such as RSA

Hybrid Encryption + Integrity

- Added integrity checks using HMACS
- Uses a key to hash the data
- Recipient can not generate hash without decrypting the session key

Digital Signatures

	Public Key	Private Key
Encryption (RSA)		
Digital Signatures		

Digital Signatures

	Public Key	Private Key
Encryption (RSA)	Encrypt	Decrypt
Digital Signatures	Verify Signature	Sign Message

Digital Signatures in the .NET Framework

- Digital signatures use 3 main classes
  - RSACryptoServiceProvider
  - RSAPKCS1SignatureFormatter
  - RSAPKCS1SignatureDeformatter

Using SecureString for Sensitive Data

- System.String is not a secure solution
- System.String has the following problems
  - Several copies in memory
  - Not encrypted
  - Not mutable, old copied in memory
  - No effective way to clear out memory

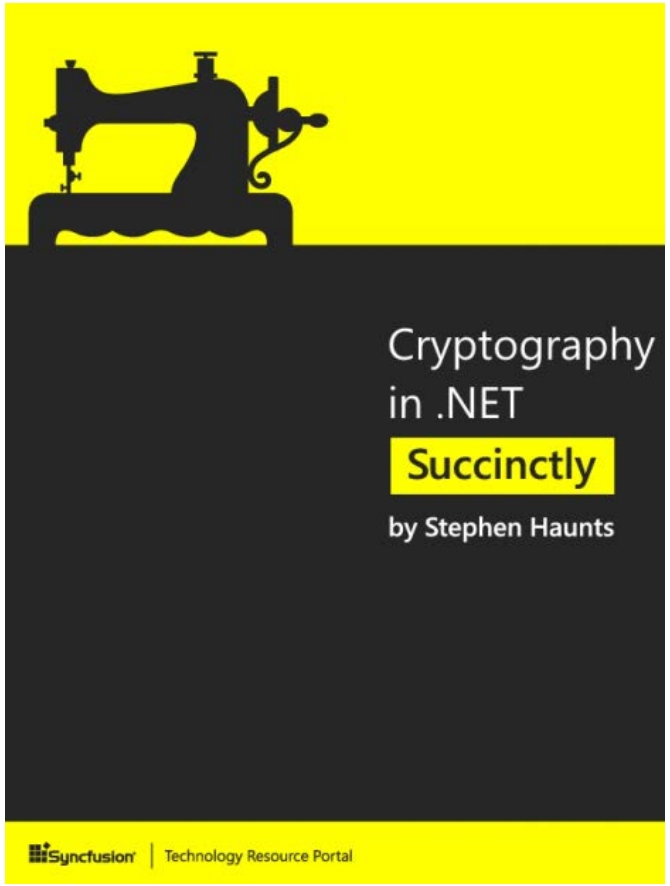
Using SecureString for Sensitive Data

- SecureString stored in encrypted memory
- SecureString implements IDisposable
- Create SecureString with a pointer to a char array

Recommended Reading List

Continuing Your Journey with Cryptography

Recommended Reading



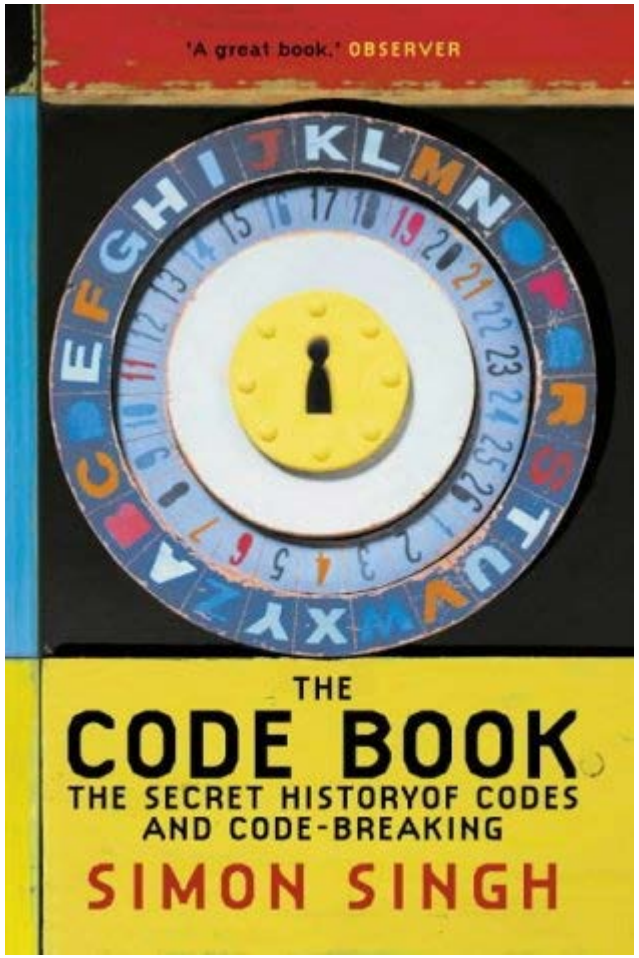
Cryptography in .NET Succinctly

Stephen Haunts

Good companion book to this course

http://bit.ly/1HePKf5

Recommended Reading

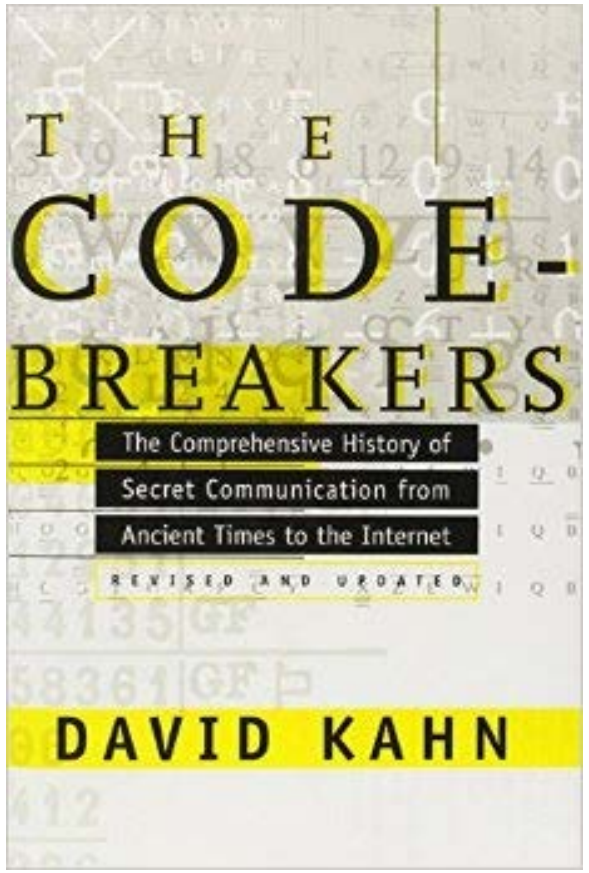


The Code Book

Simon Singh

Brief history of cryptography

Recommended Reading

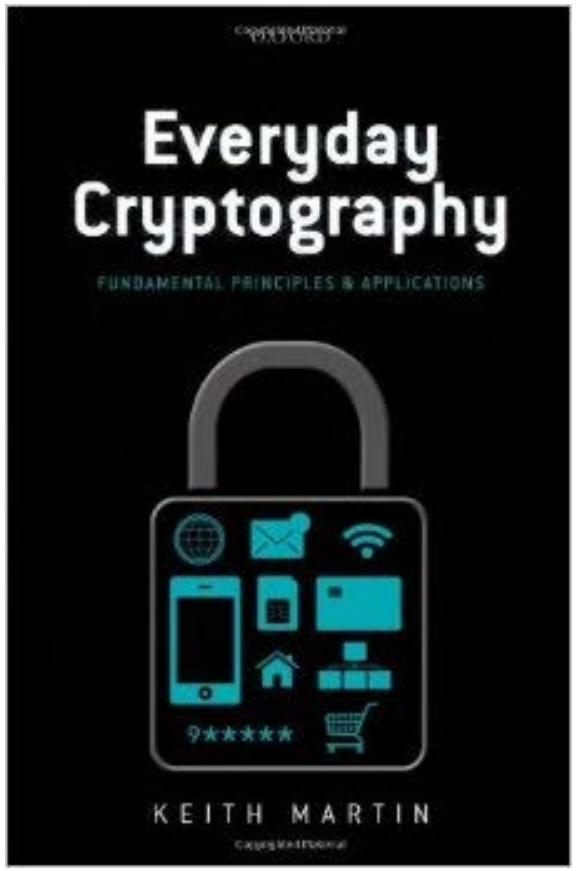


The Code Breakers

David Kahn

Detailed history of cryptography

Recommended Reading

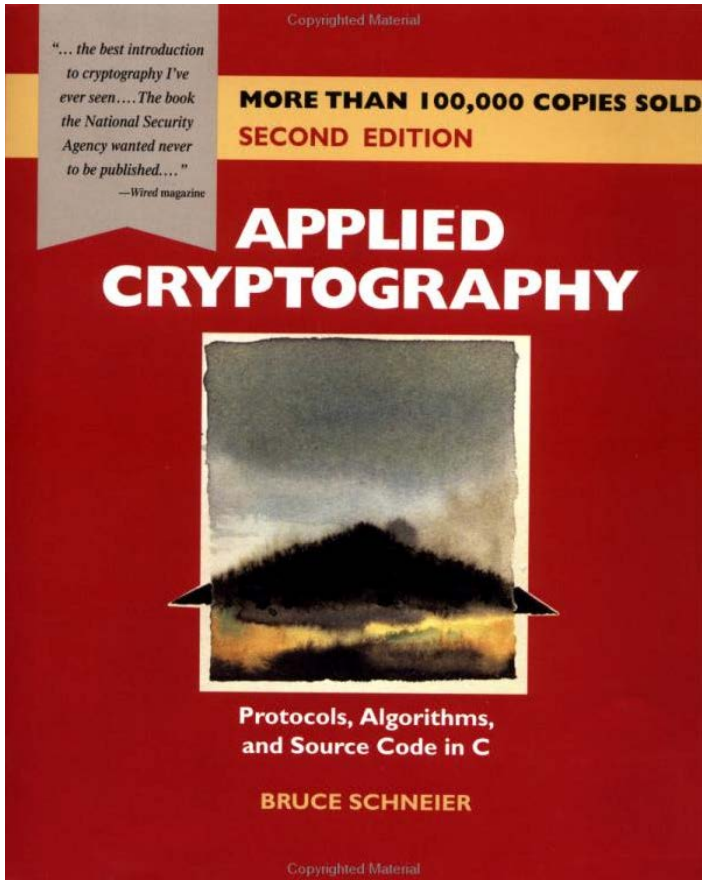


Everyday Cryptography

Keith Martin

More technical look at modern cryptography and its practical uses

Recommended Reading



Applied Cryptography

Bruce Schnier

Very technical and in-depth book about how cryptography algorithms work

Contacting Me

http://www.stephenhaunts.com