Stephen Haunts

.NET Data Security Hope is not a strategy

What is cyptography

4 pillors of cypt

Confidential

Integrity

Authentication

Non repudiation

Random Numbers

RNGCryptoserviceprovider

Hashing

4 principles of hashing

Easy to compute

Infeasible to gen a specific hash

Modify

Identical

MD5

SHA3 not in .net at the moment

SHA256

Authenticated hashing

Must have the same key as the sender

Hashing passwords

Does any one work on a system that only does a sha

Hash cracker

Hash cat

Salt password

Valid gpu may be able to crack

Rfc2898DeriveBytes

What is an acceptable time for your user to wait

Ashley Madison

Used Bcrypt for password

Stored NMD5 tokens

Symmetric encryption

Same key to encrypt and decrypt

Symmetric Algorithem

AES

Initialization vector

AESManaged

Not FIPS 197-2 certified

AESCryptoServiceProvder

Asymmetric encryption

Public key private key

RAS

2048 min standard

Only up to size of key

23 \* 17 = 391

67 \* 89 = 5963

Public 5963

Private 67 \* 89

Limit to the data size = size of key

Digital signatures

Key gen

Signing alg

Sig verif

RSAPKCS1SigatureFormatter

Hybrid encryption

Combine rsa aes into

RSA encrypt

AES

AES

HMAC

Digital signature of HMAC

Applied crypt in .Net and azure key vault

pluralsight