Cryptography

Leif Andersen

Michael Bradshaw

University of Utah

What is Encryption?

Pithy Responce

Symmetric

Vs.

Asymmetric

Symmetric

Symmetric

Message → Key → af23c2...

↑

Same key

↓

af23c2... → Key → Message

Symmetric
Vs.
Asymmetric

Asymmetric

Asymmetric

Message → Key #1 → af23c2...

↑

Different keys

↓

af23c2... → Key #2 → Message

Symmetric Cryptography

Advanteges

Advantages

- Relatively Fast

Advantages

- Relatively Fast
- Password Based Encryption

Advantages

- Relatively Fast
- Password Based Encryption
- Generally Easier to Implement

Disadvanteges

Disadvantages

- Shared Key

Disadvantages

- Shared Key
- Another disadvantage

Common Algorithms

rot13

rot13

M-x dunnet

Common Algorithms

- AES

Common Algorithms

- AES
- DES

Common Algorithms

- AES
- DES
- 3DES

Common Algorithms

- AES
- DES
- 3DES
- Blowfish

Common Algorithms

- AES
- DES
- 3DES
- Blowfish
- Twofish

Common Algorithms

- AES
- DES
- 3DES
- Blowfish
- Twofish
- Serpent

AES

- Advanced Encryption Standard

AES

- Advanced Encryption Standard
- National Institute of Standards and Technology (NIST)

AES

- Advanced Encryption Standard
- National Institute of Standards and Technology (NIST)
- Non-regulatory agency of the United States Department of Commerce

AES

- Advanced Encryption Standard
- National Institute of Standards and Technology (NIST)
- Non-regulatory agency of the United States Department of Commerce
- Rijndael Cipher

AES

- Advanced Encryption Standard

AES

- Advanced Encryption Standard
- SubBytes - Lookup table byte substition

AES

- Advanced Encryption Standard
- SubBytes - Lookup table byte substition
- ShiftRows - Circularly shifts each row differently

AES

- Advanced Encryption Standard
- SubBytes - Lookup table byte substition
- ShiftRows - Circularly shifts each row differently
- MixColums - Mix each column together with an invertible matrix

AES

- Advanced Encryption Standard
- SubBytes - Lookup table byte substition
- ShiftRows - Circularly shifts each row differently
- MixColums - Mix each column together with an invertible matrix
- AddRoundKey - Add a key from the Kijndael key schedule for the round

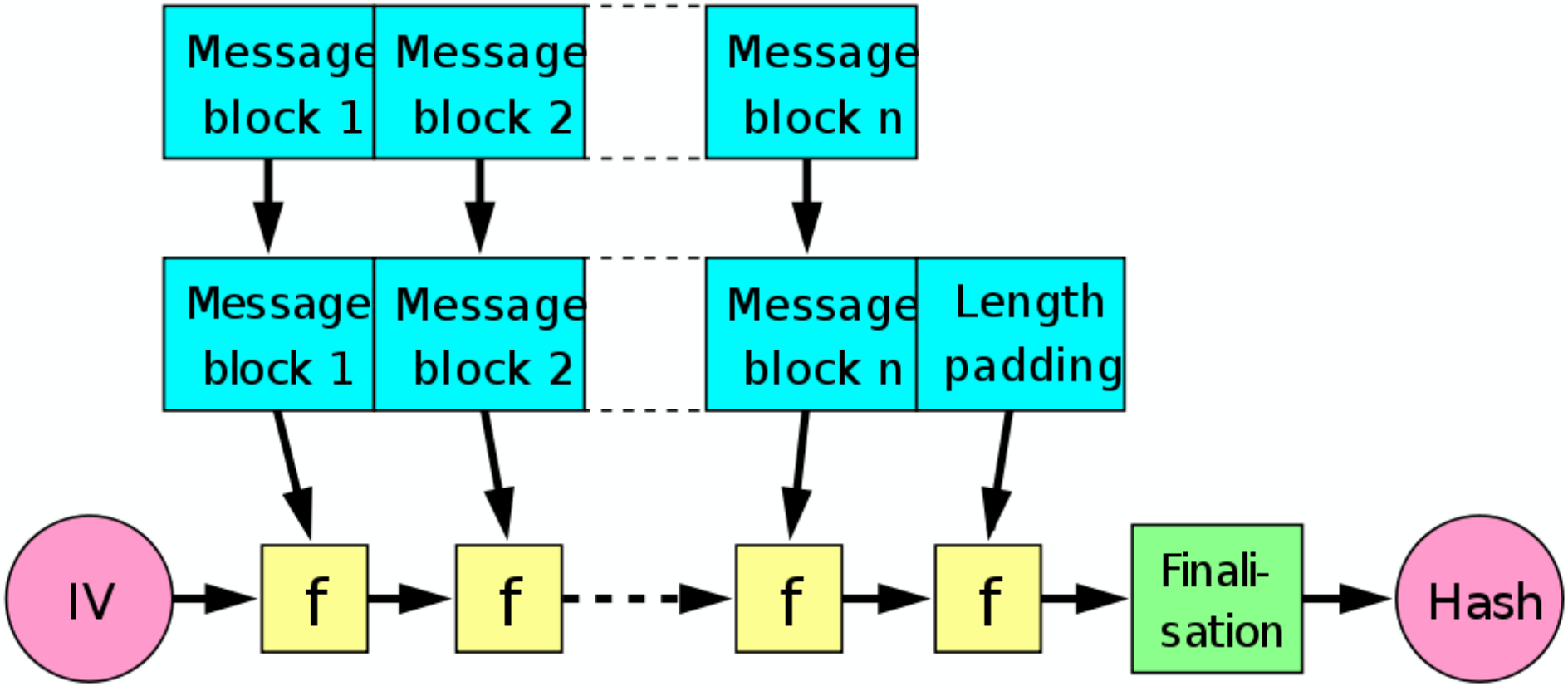
AES

- Advanced Encryption Standard
- SubBytes - Lookup table byte substition
- ShiftRows - Circularly shifts each row differently
- MixColums - Mix each column together with an invertible matrix
- AddRoundKey - Add a key from the Kijndael key schedule for the round
- Animation: http://bit.ly/5CB5m

Hashing

What is hashing?

A one way function


Message block 1
Message block 2
Message block n
Message block 1
Message block 2
Message block n
Length padding
IV
f
f
f
f
Finali-sation
Hash

Common Hash Functions

Common Hash Functions

- MD5

Common Hash Functions

- MD5
- SHA–1

Common Hash Functions

- MD5
- SHA–1
- SHA-256

Good Hashing Practices

Good Hashing Practices

- Pick a slow hash function.

Good Hashing Practices

- Pick a slow hash function.
- Hash multiple times.

Rainbow Tables

Hashing

Hashing with Salt

What is Salt?

<hash>:<salt>

How to Salt

How to Salt

- Append random characters to string.

How to Salt

- Append random characters to string.
- Hash string.

How to Salt

- Append random characters to string.
- Hash string.
- Store results of hash with random characters from salt attached.

Verify Salted Hash

Verify Salted Hash

- Read salt from database.

Verify Salted Hash

- Read salt from database.
- Append salt to string.

Verify Salted Hash

- Read salt from database.
- Append salt to string.
- Check if checksums match.

Reasons to Salt

Reasons to Salt

You Hate Rainbows


POLICE
SLCPD
Serving with Integrity

3__jordan99PDsmith@slcgov99PDcom__db8a611bd35c926f17ccd2ab4d6ec6ecdd3dad06__Jordan__Smith__PR
Specialist__jordan99PDsmith@slcgov99PDcom__801-707-6690
8__amarvel__feb051e448bb2c27f81b7b832c17806582183d8f__Aaron__Marvel__web developer
II__aaron99PDmarvel@slcgov99PDcom__801-123-4567
9__ljones__7c01b8b7981eb1fe57817f2674f280c1eb9eb633__Lara__Jones____lara99PDjones@slcgov99PDcom__
10__jwatkins__109f4b3c50d7b0df729d299bc6f8e9ef9066971f__Jared__Watkins____jared99PDwatkins@slcgov99PDcom__


Google

{SHA1}feb051e448bb2c27f81b7b832c17806582183d8f marvel

sha1('**test2**') 109f4b3c50d7b0df729d299bc6f8e9ef9066971f

FAIL!

Asymmetric Cryptography

Common Algorithms

Common Algorithms

- RSA

Common Algorithms

- RSA
- ECC

RSA

Key Generation

RSA Key Generation

Choose two numbers p and q

RSA Key Generation

$$n = pq$$

RSA Key Generation

$$\varphi(n) = \varphi(pq)$$

RSA Key Generation

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q)$$

RSA Key Generation

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q)$$
$$= (p-1)(q-1)$$

RSA Key Generation

Choose $e : 1 < e < \varphi(n)$
and $\gcd(e, \varphi(n)) = 1$

RSA Key Generation

Determine $d : d^{-1} \equiv e \pmod{\varphi(n)}$

RSA Key Generation

d is the private key.

e is the public key.

Encryption

Encryption

Convert message text M into some $m : 0 \leq m < n$

Encryption

$$c \equiv m^e \pmod{n}$$

Encryption

$$c \equiv m^e \pmod{n}$$

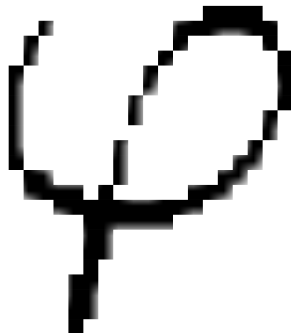
Where c is your encrypted text

Decryption

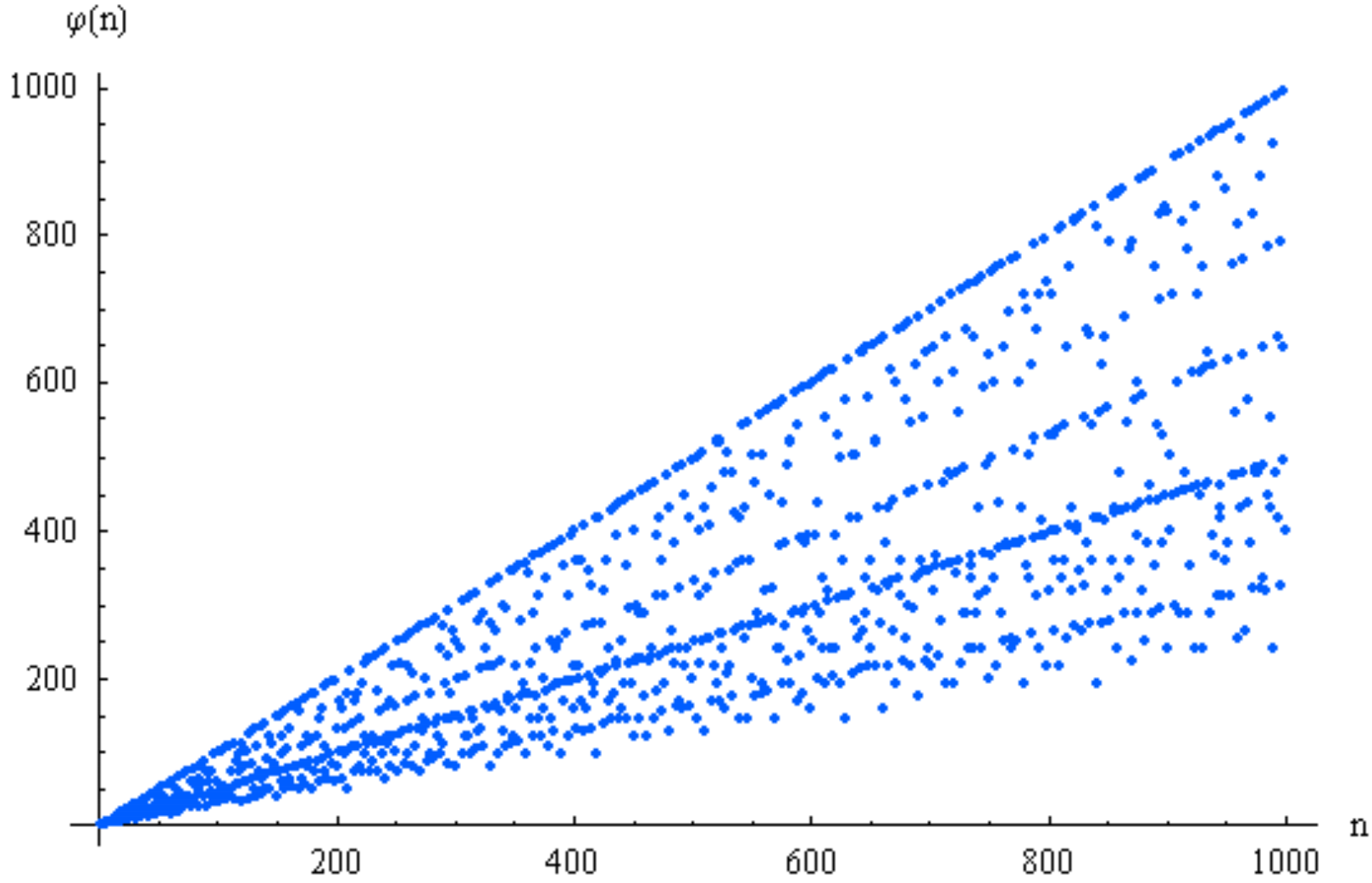
Decryption

$$e \equiv c^d \pmod{n}$$

Why is this secure?



$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

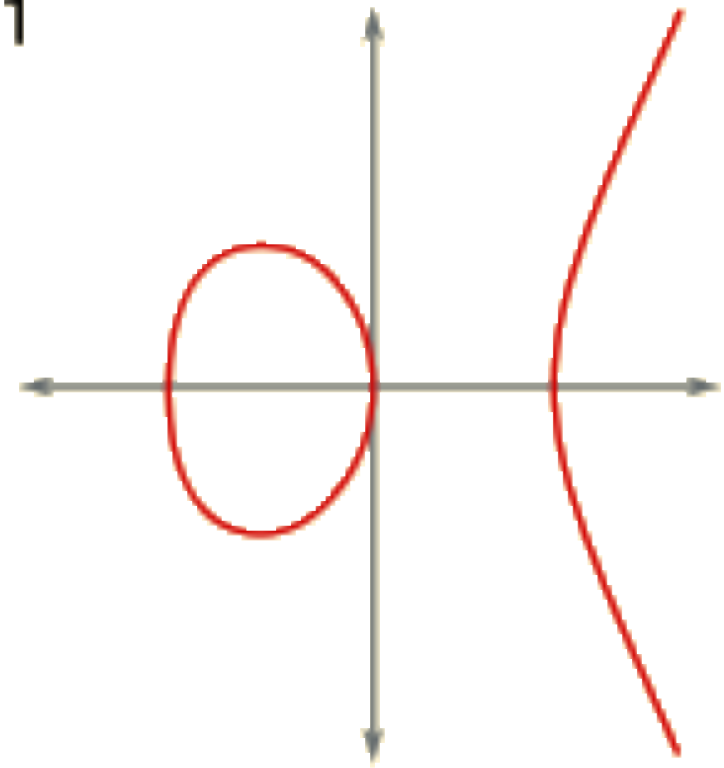

φ(n)
1000
800
600
400
200
200
400
600
800
1000
n

ECC

Elliptic Curve Cryptography

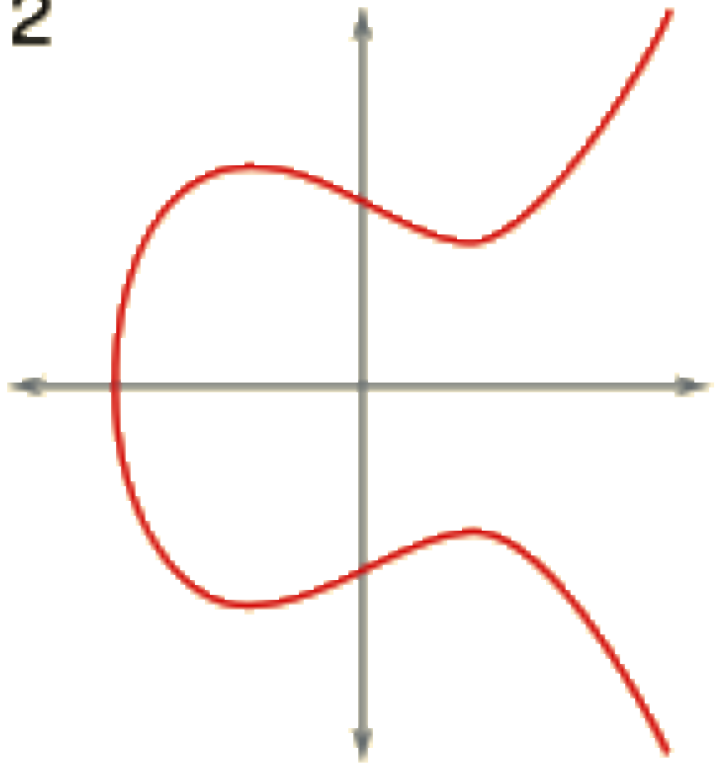
$$y^2 = x^3 + ax + b$$

1



$y^2 = x^3 - x$

2



$y^2 = x^3 - x + 1$

1011

$$1x^3 + 0x^2 + 1x + 1$$

RSA ECC

RSA < ECC

Major problem with Asymmetric Cryptography

SLOW

Solution:

Solution:

Use Symmetric Cryptography

Fast Asymmetric Cryptography

- Generate symmetric key.

Fast Asymmetric Cryptography

- Generate symmetric key.
- Encrypt data with symmetric key.

Fast Asymmetric Cryptography

- Generate symmetric key.
- Encrypt data with symmetric key.
- Encrypt symmetric key with public key.

Fast Asymmetric Cryptography

- Generate symmetric key.
- Encrypt data with symmetric key.
- Encrypt symmetric key with public key.
- Send encrypted symmetric key and data to recipient.

Fast Asymmetric Cryptography

- Generate symmetric key.
- Encrypt data with symmetric key.
- Encrypt symmetric key with public key.
- Send encrypted symmetric key and data to recipient.
- Recipient decrypts symmetric key with private key, and decrypts data with symmetric key.

Signing

Signing

- Hash Message.

Signing

- Hash Message.
- Encrypt hash with private key.

Signing

- Hash Message.
- Encrypt hash with private key.
- Send message and encrypted hash to recipient

Signing

- Hash Message.
- Encrypt hash with private key.
- Send message and encrypted hash to recipient
- Recipient decrypts hash with public key.

Signing

- Hash Message.
- Encrypt hash with private key.
- Send message and encrypted hash to recipient
- Recipient decrypts hash with public key.
- Recipient hashes message.

Signing

- Hash Message.
- Encrypt hash with private key.
- Send message and encrypted hash to recipient
- Recipient decrypts hash with public key.
- Recipient hashes message.
- If checksums match, recipient knows message came from sender.

WARNING!!!

WARNING!!!

Never encrypt something
a third party
requests encrypted.

Questions?