



Practical Aspects of Modern Cryptography

Josh Benaloh & Brian LaMacchia




Lecture 4: AES, Hash Functions, and Protocols



Advanced Encryption Standard

- ◆ Competition to replace the Data Encryption Standard (DES)
- ◆ 128-bit block size
- ◆ Key sizes of 128, 192, and 256 bits
- ◆ 15 ciphers were submitted
- ◆ 5 finalists were chosen


January 29, 2002 Practical Aspects of Modern Cryptography 3



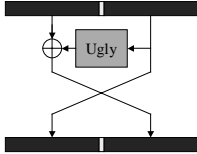
AES Finalists

- ◆ MARS (IBM submission)
- ◆ RC6 (RSA Labs submission)
- ◆ Rijndael (Joan Daemen and Vincent Rijmen)
- ◆ Serpent (Anderson, Biham, and Knudsen)
- ◆ Twofish (Schneier, et. al.)


January 29, 2002 Practical Aspects of Modern Cryptography 4



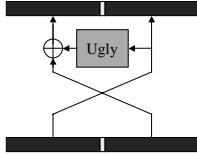
Feistel Ciphers



January 29, 2002 Practical Aspects of Modern Cryptography 5



Feistel Ciphers



January 29, 2002 Practical Aspects of Modern Cryptography 6

Feistel Ciphers

January 29, 2002 Practical Aspects of Modern Cryptography 7

AES Finalists

- ◆ MARS (IBM submission)
- ◆ RC6 (RSA Labs submission)
- ◆ Rijndael (Joan Daemen and Vincent Rijmen)
- ◆ Serpent (Anderson, Biham, and Knudsen)
- ◆ Twofish (Schneier, et. al.)

January 29, 2002 Practical Aspects of Modern Cryptography 8

Rijndael

k _{0,0}	k _{0,1}	k _{0,2}	k _{0,3}	k _{0,4}	k _{0,5}	k _{0,6}	k _{0,7}
k _{1,0}	k _{1,1}	k _{1,2}	k _{1,3}	k _{1,4}	k _{1,5}	k _{1,6}	k _{1,7}
k _{2,0}	k _{2,1}	k _{2,2}	k _{2,3}	k _{2,4}	k _{2,5}	k _{2,6}	k _{2,7}
k _{3,0}	k _{3,1}	k _{3,2}	k _{3,3}	k _{3,4}	k _{3,5}	k _{3,6}	k _{3,7}

16, 24, or 32 bytes of key

a _{0,0}	a _{0,1}	a _{0,2}	a _{0,3}	a _{0,4}	a _{0,5}	a _{0,6}	a _{0,7}
a _{1,0}	a _{1,1}	a _{1,2}	a _{1,3}	a _{1,4}	a _{1,5}	a _{1,6}	a _{1,7}
a _{2,0}	a _{2,1}	a _{2,2}	a _{2,3}	a _{2,4}	a _{2,5}	a _{2,6}	a _{2,7}
a _{3,0}	a _{3,1}	a _{3,2}	a _{3,3}	a _{3,4}	a _{3,5}	a _{3,6}	a _{3,7}

16, 24, or 32 bytes of data

January 29, 2002 Practical Aspects of Modern Cryptography 9

Rijndael

- ◆ 4 transformations per round
- ◆ ByteSub: nonlinearity
- ◆ ShiftRow: inter-column diffusion
- ◆ MixColumn: inter-byte diffusion
- ◆ Round key addition

January 29, 2002 Practical Aspects of Modern Cryptography 10

Rijndael ByteSub

a _{0,0}	a _{0,1}	a _{0,2}	a _{0,3}
a _{1,0}	a _{1,1}	a _{1,2}	a _{1,3}
a _{2,0}	a _{2,1}	a _{2,2}	a _{2,3}
a _{3,0}	a _{3,1}	a _{3,2}	a _{3,3}

⇒

b _{0,0}	b _{0,1}	b _{0,2}	b _{0,3}
b _{1,0}	b _{1,1}	b _{1,2}	b _{1,3}
b _{2,0}	b _{2,1}	b _{2,2}	b _{2,3}
b _{3,0}	b _{3,1}	b _{3,2}	b _{3,3}

A single 8-bit to 8-bit (invertible) S-box is applied to each byte.

January 29, 2002 Practical Aspects of Modern Cryptography 11

Rijndael MixColumn

a _{0,0}	a _{0,1}	a _{0,2}	a _{0,3}
a _{1,0}	a _{1,1}	a _{1,2}	a _{1,3}
a _{2,0}	a _{2,1}	a _{2,2}	a _{2,3}
a _{3,0}	a _{3,1}	a _{3,2}	a _{3,3}

⇒

b _{0,0}	b _{0,1}	b _{0,2}	b _{0,3}
b _{1,0}	b _{1,1}	b _{1,2}	b _{1,3}
b _{2,0}	b _{2,1}	b _{2,2}	b _{2,3}
b _{3,0}	b _{3,1}	b _{3,2}	b _{3,3}

An (invertible) linear transform is applied to each column.

January 29, 2002 Practical Aspects of Modern Cryptography 12

Rijndael ShiftRow

An different cyclic shift is applied to each row.

January 29, 2002 Practical Aspects of Modern Cryptography 13

Rijndael Round key addition

The round key is XORed to complete the round.

January 29, 2002 Practical Aspects of Modern Cryptography 14

Rijndael Key Schedule

The key schedule is defined on 4-byte words by

Round key 0	Round key 1	Round key 2	...
-------------	-------------	-------------	-----

- ◆ $k_i = k_{i-4} \otimes k_{i-1}$ when i is not a multiple of 4
- ◆ $k_i = k_{i-4} \otimes f(k_{i-1})$ when i is a multiple of 4

January 29, 2002 Practical Aspects of Modern Cryptography 15

Cipher Integrity

- ◆ When using block ciphers in CBC mode, there is generally a built-in integrity check.
- ◆ However, when using block ciphers in ECB mode or (especially) when using stream ciphers, an external integrity check is crucial.
- ◆ Such an integrity check is called a Message Authentication Code (MAC).

January 29, 2002 Practical Aspects of Modern Cryptography 16

Stream Cipher Integrity

- ◆ It is easy for an adversary (even one who can't decrypt the ciphertext) to alter the plaintext in a known way.

Bob to Bob's Bank: Please transfer \$0,000,002.00 to the account of my good friend Alice.

January 29, 2002 Practical Aspects of Modern Cryptography 17

Stream Cipher Integrity

- ◆ It is easy for an adversary (even one who can't decrypt the ciphertext) to alter the plaintext in a known way.

Bob to Bob's Bank: Please transfer \$1,000,002.00 to the account of my good friend Alice.

January 29, 2002 Practical Aspects of Modern Cryptography 18

One-Way Hash Functions

- ◆ The idea of a *check sum* is great, but it is designed to prevent accidental changes in a message.
- ◆ For cryptographic integrity, we need an integrity check that is resilient against a smart and determined adversary.

January 29, 2002 Practical Aspects of Modern Cryptography 19

One-Way Hash Functions

Generally, a *one-way hash function* is a function $H : \{0,1\}^* \rightarrow \{0,1\}^k$ (typically k is 128 or 160) such that given an input value x , one cannot find a value $x' \neq x$ such $H(x) = H(x')$.

January 29, 2002 Practical Aspects of Modern Cryptography 20

One-Way Hash Functions

There are many measures for one-way hashes.

- ◆ Non-invertability: given y , it's difficult to find any x such that $H(x) = y$.
- ◆ Collision-intractability: one cannot find a pair of values $x' \neq x$ such that $H(x) = H(x')$.

January 29, 2002 Practical Aspects of Modern Cryptography 21

An Example Hash: SHA-1

- ◆ SHA-1 was designed by the US Government as part of the Digital Signature Standard.
- ◆ SHA-1 is the most-commonly used hash function today.
 - It's the hash function in which we have the most faith right now.
- ◆ SHA-1 takes any size input and produces a 160-bit output (the digest value).

January 29, 2002 Practical Aspects of Modern Cryptography 22

A Cryptographic Hash: SHA-1

Diagram illustrating a SHA-1 compression function. A 512-bit input and an initial value (IV) are fed into a trapezoidal block labeled "Compression Function". The output is a 160-bit Output.

January 29, 2002 Practical Aspects of Modern Cryptography 23

A Cryptographic Hash: SHA-1

Diagram illustrating one of 80 rounds of SHA-1 processing. A 512-bit input is split into eight 64-bit blocks. Each block is processed by a function that produces a 160-bit output.

January 29, 2002 Practical Aspects of Modern Cryptography 24

A Cryptographic Hash: SHA-1

160-bit ↓ 512-bit ↓

No Change

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 25

A Cryptographic Hash: SHA-1

160-bit ↓ 512-bit ↓

Rotate 30 bits

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 26

A Cryptographic Hash: SHA-1

160-bit ↓ 512-bit ↓

No Change

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 27

A Cryptographic Hash: SHA-1

160-bit ↓ 512-bit ↓

No Change

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 28

A Cryptographic Hash: SHA-1

160-bit ↓ 512-bit ↓

?

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 29

A Cryptographic Hash: SHA-1

What's in the final 32-bit transform?

- ◆ Take the rightmost word.
- ◆ Add in the leftmost word rotated 5 bits.
- ◆ Add in a round-dependent function f of the middle three words.

January 29, 2002 Practical Aspects of Modern Cryptography 30

A Cryptographic Hash: SHA-1

160-bit 512-bit

One of 80 rounds

January 29, 2002 Practical Aspects of Modern Cryptography 31

A Cryptographic Hash: SHA-1

Depending on the round, the “non-linear” function f is one of the following.

$$f(X, Y, Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$$

$$f(X, Y, Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$$

$$f(X, Y, Z) = X \oplus Y \oplus Z$$

January 29, 2002 Practical Aspects of Modern Cryptography 32

A Cryptographic Hash: SHA-1

What’s in the final 32-bit transform?

- ◆ Take the rightmost word.
- ◆ Add in the leftmost word rotated 5 bits.
- ◆ Add in a round-dependent function f of the middle three words.

January 29, 2002 Practical Aspects of Modern Cryptography 33

A Cryptographic Hash: SHA-1

What’s in the final 32-bit transform?

- ◆ Take the rightmost word.
- ◆ Add in the leftmost word rotated 5 bits.
- ◆ Add in a round-dependent function f of the middle three words.
- ◆ Add in a round-dependent constant.

January 29, 2002 Practical Aspects of Modern Cryptography 34

A Cryptographic Hash: SHA-1

What’s in the final 32-bit transform?

- ◆ Take the rightmost word.
- ◆ Add in the leftmost word rotated 5 bits.
- ◆ Add in a round-dependent function f of the middle three words.
- ◆ Add in a round-dependent constant.
- ◆ Add in a portion of the 512-bit message.


January 29, 2002 Practical Aspects of Modern Cryptography 35

A Cryptographic Hash: SHA-1

160-bit 512-bit

One of 80 rounds


January 29, 2002 Practical Aspects of Modern Cryptography 36



One-Way Hash Functions

- ◆ When using a stream cipher, a (keyed) hash of the message can be appended to ensure integrity. [Message Authentication Code]
- ◆ When forming a digital signature, the signature need only be applied to a hash of the message. [Message Digest]


January 29, 2002 Practical Aspects of Modern Cryptography 37



Cryptographic Tools

- One-Way Trapdoor Functions
- Public-Key Encryption Schemes
- One-Way Permutations
- One-Way Functions
- One-Way Hash Functions
- Pseudo-Random Number-Generators
- Secret-Key Encryption Schemes
- Digital Signature Schemes


January 29, 2002 Practical Aspects of Modern Cryptography 38



Using Public Key Encryption

Now that we have all of these tools available, how do we actually send a (short) message, perhaps a symmetric key, encrypted with a public key?

January 29, 2002 Practical Aspects of Modern Cryptography 39



PKCS#1 v1 Message Format:

Recall the Bleichenbacher attack


00 01 XX XX ... XX 00 YY YY ... YY

random message

non-zero

bytes

January 29, 2002 Practical Aspects of Modern Cryptography 40




OAEP

Optimal Asymmetric Encryption Protocol

To encrypt the message M ,
 Select a random value r ,
 For a PRNG G and one-way hash H , use the public key to encrypt the following:

$$M \otimes G(r) \parallel r \otimes H(M \otimes G(r))$$

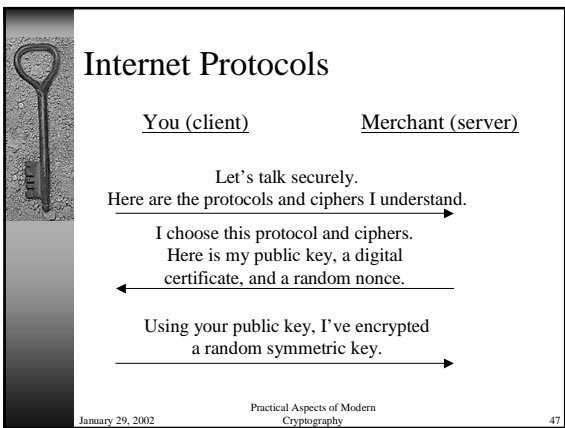
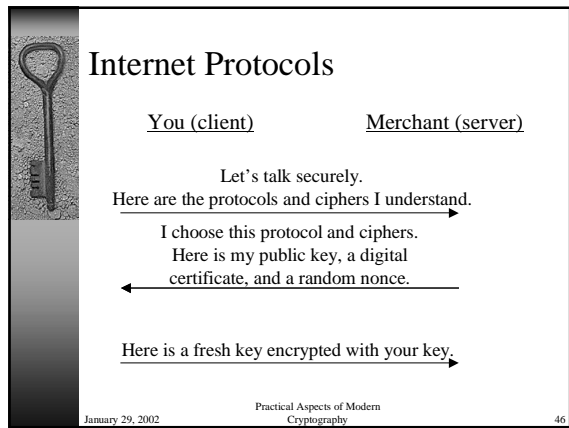
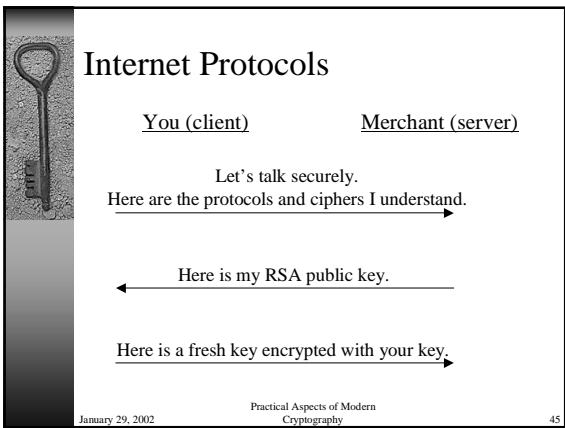
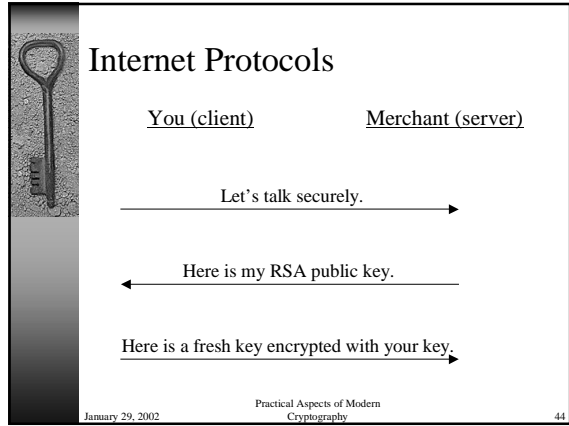
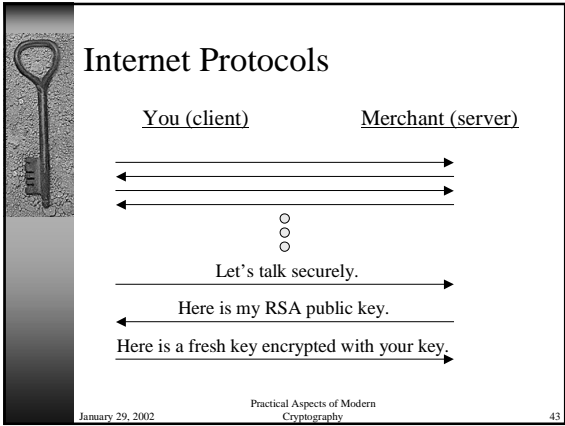
January 29, 2002 Practical Aspects of Modern Cryptography 41



Internet Protocols

- ◆ 1994: Secure Sockets Layer (SSL) V2.0
- ◆ 1995: Private Communication Technology (PCT) V1.0
- ◆ 1996: Secure Sockets Layer (SSL) V3.0
- ◆ 1997: Private Communication Technology (PCT) V4.0
- ◆ 1999: Transport Layer Security (TLS) V1.0

January 29, 2002 Practical Aspects of Modern Cryptography 42



Internet Protocols

All subsequent secure messages are sent using the symmetric key and a keyed hash for message authentication.

January 29, 2002 Practical Aspects of Modern Cryptography 48