


# Practical Aspects of Modern Cryptography


Josh Benaloh & Brian LaMacchia



## Public-Key History

- ◆ 1976 *New Directions in Cryptography*  
**Whit Diffie and Marty Hellman**
  - One-Way functions
  - Diffie-Hellman Key Exchange
- ◆ 1978 RSA paper  
**Ron Rivest, Adi Shamir, and Len Adleman**
  - RSA Encryption System
  - RSA Digital Signature Mechanism


January 15, 2002 Practical Aspects of Modern Cryptography



## The Fundamental Equation

$$Z = Y^X \pmod N$$

January 15, 2002 Practical Aspects of Modern Cryptography

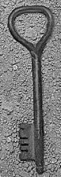


## Diffie-Hellman

$$Z = Y^X \pmod N$$

When X is unknown, the problem is known as the *discrete logarithm* and is generally believed to be hard to solve.

January 15, 2002 Practical Aspects of Modern Cryptography




## Diffie-Hellman Key Exchange

<p><u>Alice</u></p> <ul style="list-style-type: none"> <li>◆ Randomly select a large integer <math>a</math> and send <math>A = Y^a \pmod N</math>.</li> <li>◆ Compute the key <math>K = B^a \pmod N</math>.</li> </ul>	<p><u>Bob</u></p> <ul style="list-style-type: none"> <li>◆ Randomly select a large integer <math>b</math> and send <math>B = Y^b \pmod N</math>.</li> <li>◆ Compute the key <math>K = A^b \pmod N</math>.</li> </ul>
--	--

$$B^a = Y^{ba} = Y^{ab} = A^b$$

January 15, 2002 Practical Aspects of Modern Cryptography



## Diffie-Hellman Key Exchange

What does Eve see?

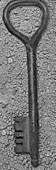
$Y, Y^a, Y^b$

... but the exchanged key is  $Y^{ab}$ .

*Belief:* Given  $Y, Y^a, Y^b$  it is difficult to compute  $Y^{ab}$ .

*Contrast with discrete logarithm assumption:*  
Given  $Y, Y^x$  it is difficult to compute  $x$ .

January 15, 2002 Practical Aspects of Modern Cryptography




## One-Way Trap-Door Functions

$$Z = Y^X \pmod N$$

Recall that this equation is solvable for  $Y$  if the factorization of  $N$  is known, but is *believed* to be hard otherwise.

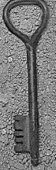
January 15, 2002 Practical Aspects of Modern Cryptography



## RSA Public-Key Cryptosystem

<p><u>Alice</u></p> <ul style="list-style-type: none"> <li>◆ Select two large random primes <math>P</math> &amp; <math>Q</math>.</li> <li>◆ Publish the product <math>N=PQ</math>.</li> <li>◆ Use <u>knowledge of <math>P</math> &amp; <math>Q</math></u> to compute <math>Y</math>.</li> </ul>	<p><u>Anyone</u></p> <ul style="list-style-type: none"> <li>◆ To send message <math>Y</math> to Alice, compute <math>Z=Y^X \pmod N</math>.</li> <li>◆ Send <math>Z</math> and <math>X</math> to Alice.</li> </ul>
---	---

January 15, 2002 Practical Aspects of Modern Cryptography



## Some RSA Details


When  $N=PQ$  is the product of distinct primes,

$$Y^X \pmod N = Y$$

whenever

$$X \pmod{(P-1)(Q-1)} = 1 \text{ and } 0 \leq Y < N.$$

January 15, 2002 Practical Aspects of Modern Cryptography



## Some RSA Details

When  $N=PQ$  is the product of distinct primes,


$$Y^X \pmod N = Y$$

whenever

$$X \pmod{(P-1)(Q-1)} = 1 \text{ and } 0 \leq Y < N.$$

Alice can easily select integers  $E$  and  $D$  such that  $E \cdot D \pmod{(P-1)(Q-1)} = 1$ .

January 15, 2002 Practical Aspects of Modern Cryptography




## Some RSA Details

Encryption:  $E(Y) = Y^E \pmod N$ .  
 Decryption:  $D(Y) = Y^D \pmod N$ .

$$\begin{aligned}
 D(E(Y)) &= (Y^E \pmod N)^D \pmod N \\
 &= Y^{ED} \pmod N \\
 &= Y
 \end{aligned}$$

January 15, 2002 Practical Aspects of Modern Cryptography



## RSA Signatures

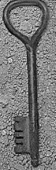
An additional property

$$D(E(Y)) = Y^{ED} \pmod N = Y$$

$$E(D(Y)) = Y^{DE} \pmod N = Y$$

Only Alice (knowing the factorization of  $N$ ) knows  $D$ . Hence only Alice can compute  $D(Y) = Y^D \pmod N$ .  
 This  $D(Y)$  serves as Alice's signature on  $Y$ .

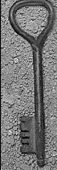
January 15, 2002 Practical Aspects of Modern Cryptography



## Remaining RSA Basics

- ◆ Why is  $Y^X \bmod PQ = Y$  whenever  $X \bmod (P-1)(Q-1) = 1$ ,  $0 \leq Y < PQ$ , and  $P$  and  $Q$  are distinct primes?
- ◆ How can Alice can select integers  $E$  and  $D$  such that  $E \cdot D \bmod (P-1)(Q-1) = 1$ ?


January 15, 2002 Practical Aspects of Modern Cryptography



## Modular Arithmetic

- ◆ To compute  $(A+B) \bmod N$ , compute  $(A+B)$  and take the result mod  $N$ .
- ◆ To compute  $(A-B) \bmod N$ , compute  $(A-B)$  and take the result mod  $N$ .
- ◆ To compute  $(A \times B) \bmod N$ , compute  $(A \times B)$  and take the result mod  $N$ .
- ◆ To compute  $(A \div B) \bmod N$ , ...

January 15, 2002 Practical Aspects of Modern Cryptography



## Modular Division

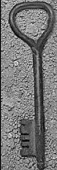
What is the value of  $(1 \div 2) \bmod 7$ ?

We need a solution to  $2x \bmod 7 = 1$ .  
Try  $x = 4$ .

What is the value of  $(7 \div 5) \bmod 11$ ?

We need a solution to  $5x \bmod 11 = 7$ .  
Try  $x = 8$ .

January 15, 2002 Practical Aspects of Modern Cryptography

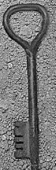


## Modular Division

Is modular division always well-defined?  
 $(1 \div 3) \bmod 6 = ?$   
 $3x \bmod 6 = 1$  has no solution!

Fact  
 $(A \div B) \bmod N$  always has a solution when  $\gcd(B, N) = 1$ .

January 15, 2002 Practical Aspects of Modern Cryptography

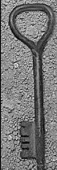


## Greatest Common Divisors

$\gcd(A, B) = \gcd(B, A - B)$   
 $\gcd(21, 12) = \gcd(12, 9) = \gcd(9, 3)$   
 $= \gcd(6, 3) = \gcd(3, 3) = \gcd(0, 3) = 3$

$\gcd(A, B) = \gcd(B, A \bmod B)$   
 $\gcd(21, 12) = \gcd(12, 9) = \gcd(9, 3)$   
 $= \gcd(0, 3) = 3$

January 15, 2002 Practical Aspects of Modern Cryptography




## Extended Euclidean Algorithm

Given integers  $A$  and  $B$ , find integers  $X$  and  $Y$  such that  $AX + BY = \gcd(A, B)$ .

When  $\gcd(A, B) = 1$ , solve  $AX \bmod B = 1$ , by finding  $X$  and  $Y$  such that  $AX + BY = \gcd(A, B) = 1$ .

Compute  $(C \div A) \bmod B$  as  $C \times (1 \div A) \bmod B$ .

January 15, 2002 Practical Aspects of Modern Cryptography



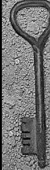
## Extended Euclidean Algorithm

Given  $A, B > 0$ , set  $x_1=1, x_2=0, y_1=0, y_2=1,$   
 $a_1=A, b_1=B, i=1.$

Repeat while  $b_i > 0$ :  $\{i = i + 1;$   
 $q = a_{i-1} \text{ div } b_{i-1}; b_i = a_{i-1} - qb_{i-1}; a_i = b_{i-1};$   
 $x_{i+1} = x_{i-1} - qx_i; y_{i+1} = y_{i-1} - qy_i\}.$

$Ax_i + By_i = a_i = \text{gcd}(A, B).$


January 15, 2002 Practical Aspects of Modern  
Cryptography



## Remaining RSA Basics

- ◆ Why is  $Y^X \text{ mod } PQ = Y$  whenever  
 $X \text{ mod } (P-1)(Q-1) = 1, 0 \leq Y < PQ,$   
and  $P$  and  $Q$  are distinct primes?
- ◆ How can Alice can select integers  $E$  and  $D$   
such that  $E \cdot D \text{ mod } (P-1)(Q-1) = 1$ ?

January 15, 2002 Practical Aspects of Modern  
Cryptography



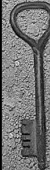
## Fermat's Little Theorem

If  $p$  is prime,  
then  $x^{p-1} \text{ mod } p = 1$  for all  $0 < x < p.$

Equivalently ...

If  $p$  is prime,  
then  $x^p \text{ mod } p = x \text{ mod } p$  for all integers  $x.$

January 15, 2002 Practical Aspects of Modern  
Cryptography



## Proof of Fermat's Little Theorem


### The Binomial Theorem

$$(x + y)^p = x^p + \binom{p}{1}x^{p-1}y + \dots + \binom{p}{p-1}xy^{p-1} + y^p$$

If  $p$  is prime, then  $\binom{p}{i} \text{ mod } p = 0$  for  $0 < i < p.$

Thus,  $(x + y)^p \text{ mod } p = (x^p + y^p) \text{ mod } p.$

January 15, 2002 Practical Aspects of Modern  
Cryptography



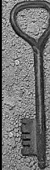
## Proof of Fermat's Little Theorem

By induction on  $x \dots$

### Basis

If  $x = 0$ , then  $x^p \text{ mod } p = 0 = x \text{ mod } p.$   
If  $x = 1$ , then  $x^p \text{ mod } p = 1 = x \text{ mod } p.$

January 15, 2002 Practical Aspects of Modern  
Cryptography

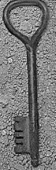


## Proof of Fermat's Little Theorem

### Inductive Step

Assume that  $x^p \text{ mod } p = x \text{ mod } p.$   
Then  $(x + 1)^p \text{ mod } p = (x^p + 1^p) \text{ mod } p$   
 $= (x + 1) \text{ mod } p.$   
Hence,  $x^p \text{ mod } p = x \text{ mod } p$  for integers  $x \geq 0.$   
Also true for negative  $x$ , since  $(-x)^p = (-1)^p x^p.$

January 15, 2002 Practical Aspects of Modern  
Cryptography



## Proof of RSA

We have shown ...

$$Y^P \bmod P = Y \text{ whenever } 0 \leq Y < P$$

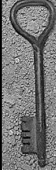
and  $P$  is *prime*!

You will show ...

$$Y^{K(P-1)(Q-1)+1} \bmod PQ = Y \text{ when } 0 \leq Y < PQ$$

$P$  and  $Q$  are distinct primes and  $K \geq 0$ .

January 15, 2002 Practical Aspects of Modern  
Cryptography




## Authentication

How can I use RSA to *authenticate* someone's identity?

If Alice's public key  $E_A$ , just pick a random message  $m$  and send  $E_A(m)$ .

If  $m$  comes back, I must be talking to Alice.

January 15, 2002 Practical Aspects of Modern  
Cryptography



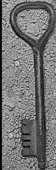
## Authentication

Should Alice be happy with this method of authentication?

Bob sends Alice the authentication string  $y = \text{"I owe Bob \$1,000,000 - signed Alice."}$

Alice dutifully authenticates herself by decrypting (putting her signature on)  $y$ .

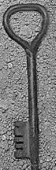
January 15, 2002 Practical Aspects of Modern  
Cryptography



## Authentication

What if Alice only returns authentication queries when the decryption has a certain format?

January 15, 2002 Practical Aspects of Modern  
Cryptography

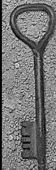


## RSA Cautions

Is it reasonable to sign/decrypt something given to you by someone else?

Note that RSA is multiplicative. Can this property be used/abused?

January 15, 2002 Practical Aspects of Modern  
Cryptography




## RSA Cautions

$$D(Y_1) \cdot D(Y_2) = D(Y_1 \cdot Y_2)$$

Thus, if I've decrypted (or signed)  $Y_1$  and  $Y_2$ , I've also decrypted (or signed)  $Y_1 \cdot Y_2$ .

January 15, 2002 Practical Aspects of Modern  
Cryptography



## The Hastad Attack

Given


$$E_1(x) = x^3 \pmod{n_1}$$

$$E_2(x) = x^3 \pmod{n_2}$$

$$E_3(x) = x^3 \pmod{n_3}$$

one can easily compute  $x$ .

January 15, 2002 Practical Aspects of Modern Cryptography




## The Bleichenbacher Attack

PKCS#1 Message Format:

$$00\ 01\ \underbrace{XX\ XX\ \dots\ XX}_{\text{random non-zero bytes}}\ 00\ \underbrace{YY\ YY\ \dots\ YY}_{\text{message}}$$

January 15, 2002 Practical Aspects of Modern Cryptography




## “Man-in-the-Middle” Attacks

Alice  $\longleftrightarrow$  Bob

Alice  $\longleftrightarrow$  Eve  $\longleftrightarrow$  Bob


January 15, 2002 Practical Aspects of Modern Cryptography



## The Practical Side

- ◆ RSA can be used to encrypt any data.
- ◆ Public-key (asymmetric) cryptography is very inefficient when compared to traditional private-key (symmetric) cryptography.

January 15, 2002 Practical Aspects of Modern Cryptography




## The Practical Side

For efficiency, one generally uses RSA (or another public-key algorithm) to transmit a private (symmetric) key.

The private *session* key is used to encrypt and authenticate any subsequent data.

Digital signatures are only used to sign a *digest* of the message.

January 15, 2002 Practical Aspects of Modern Cryptography



## Symmetric Ciphers

Private-key (symmetric) ciphers are usually divided into two classes.

- ◆ Block ciphers
- ◆ Stream ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

## Symmetric Ciphers

Private-key (symmetric) ciphers are usually divided into two classes.

- ◆ Block ciphers
- ◆ Stream ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Ciphers

Currently usually 8 bytes.  
Soon 16-32 bytes.

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Cipher Modes

Electronic Code Book (ECB) Encryption:

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Cipher Modes

Electronic Code Book (ECB) Decryption:

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Cipher Modes

Electronic Code Book (ECB) Encryption:

January 15, 2002 Practical Aspects of Modern Cryptography

## Block Cipher Modes

### Cipher Block Chaining (CBC) Encryption:

The diagram illustrates the CBC encryption process. It shows a sequence of four plaintext blocks being processed by 'Block Cipher' units. The first block is XORed with an Initialization Vector (IV). The output of each block cipher is XORed with the next plaintext block before it is processed by the next block cipher. The final output is a sequence of ciphertext blocks.

January 15, 2002  
Practical Aspects of Modern Cryptography

## Block Cipher Modes

### Cipher Block Chaining (CBC) Decryption:

The diagram illustrates the CBC decryption process. It shows a sequence of four ciphertext blocks being processed by 'Inverse Cipher' units. The first block is XORed with an Initialization Vector (IV). The output of each inverse cipher is XORed with the next ciphertext block before it is processed by the next inverse cipher. The final output is a sequence of plaintext blocks.

January 15, 2002  
Practical Aspects of Modern Cryptography

## Block Cipher Modes

### Cipher Block Chaining (CBC) Encryption:

This diagram is identical to the one in the top-left slide, showing the CBC encryption process where each plaintext block is XORed with the previous ciphertext block (or IV) before being encrypted by a block cipher.

January 15, 2002  
Practical Aspects of Modern Cryptography

## How to Build a Block Cipher

The diagram shows a single block cipher building block. It takes a 'Plaintext' block and a 'Key' as input and produces a 'Ciphertext' block as output. The block is represented as a grey box labeled 'Block Cipher'.

January 15, 2002  
Practical Aspects of Modern Cryptography

## Feistel Ciphers

The diagram shows the internal structure of a Feistel cipher. It consists of two horizontal bars representing the left and right halves of the data. An 'Ugly' function block is applied to the right half. The output of the 'Ugly' function is XORed with the left half. The two halves are then swapped.

January 15, 2002  
Practical Aspects of Modern Cryptography

## Feistel Ciphers

This diagram is identical to the one in the bottom-left slide, showing the Feistel cipher structure with an 'Ugly' function block and XOR operation between the halves.

January 15, 2002  
Practical Aspects of Modern Cryptography



### Feistel Ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

### Feistel Ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

### Feistel Ciphers

January 15, 2002 Practical Aspects of Modern Cryptography

### Feistel Ciphers

- ◆ Typically, most Feistel ciphers are iterated for about 16 rounds.
- ◆ Different “sub-keys” are used for each round.
- ◆ Even a weak round function can yield a strong Feistel cipher if iterated sufficiently.

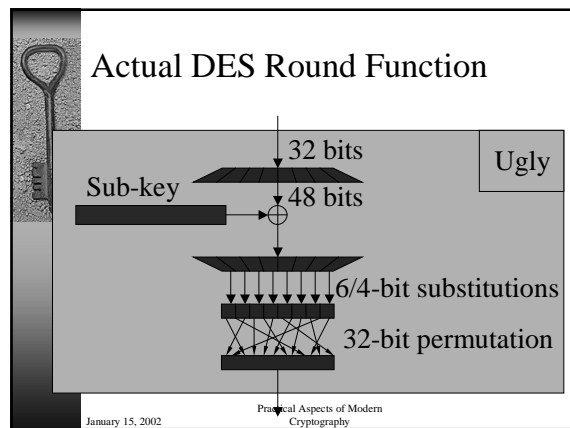
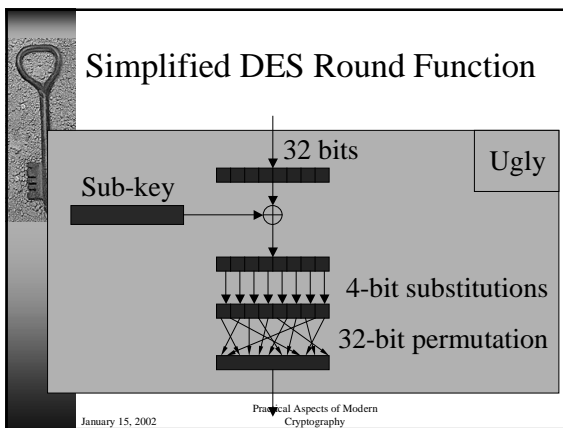
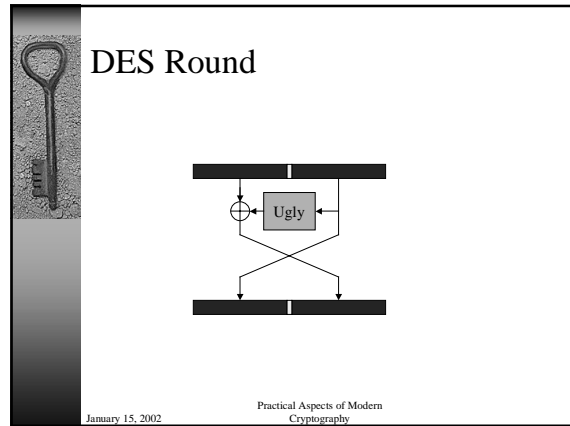
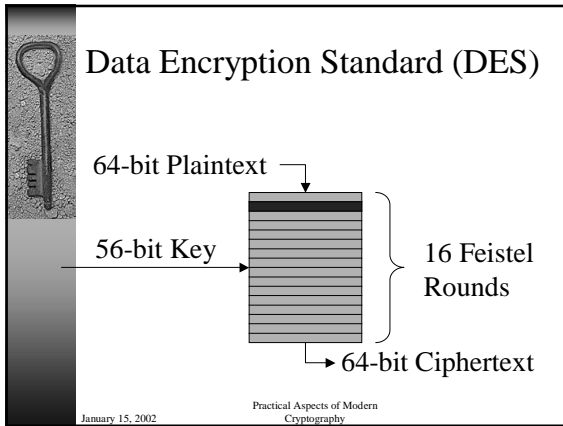
January 15, 2002 Practical Aspects of Modern Cryptography

### Data Encryption Standard (DES)

January 15, 2002 Practical Aspects of Modern Cryptography

### Data Encryption Standard (DES)

January 15, 2002 Practical Aspects of Modern Cryptography



## Symmetric Ciphers

Private-key (symmetric) ciphers are usually divided into two classes.

- ◆ Block ciphers
- ◆ Stream ciphers

January 15, 2002  
Practical Aspects of Modern Cryptography

## Stream Ciphers

- ◆ Use the key as a seed to a pseudo-random number-generator.
- ◆ Take the stream of output bits from the PRNG and XOR it with the plaintext to form the ciphertext.

January 15, 2002  
Practical Aspects of Modern Cryptography

### Stream Cipher Encryption

Plaintext:

PRNG(seed):

Ciphertext:

Practical Aspects of Modern  
Cryptography  
January 15, 2002

### Stream Cipher Decryption

Plaintext:

PRNG(seed):

Ciphertext:

Practical Aspects of Modern  
Cryptography  
January 15, 2002

### A PRNG: Alleged RC4

Initialization  
 $S[0..255] = 0, 1, \dots, 255$   
 $K[0..255] = \text{Key}, \text{Key}, \text{Key}, \dots$   
 for  $i = 0$  to  $255$   
 $j = (j + S[i] + K[i]) \bmod 256$   
 swap  $S[i]$  and  $S[j]$

Practical Aspects of Modern  
Cryptography  
January 15, 2002

### A PRNG: Alleged RC4

Iteration  
 $i = (i + 1) \bmod 256$   
 $j = (j + S[i]) \bmod 256$   
 swap  $S[i]$  and  $S[j]$   
 $t = (S[i] + S[j]) \bmod 256$   
 Output  $S[t]$

Practical Aspects of Modern  
Cryptography  
January 15, 2002

### 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.

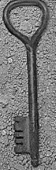
Practical Aspects of Modern  
Cryptography  
January 15, 2002

### 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.

Practical Aspects of Modern  
Cryptography  
January 15, 2002



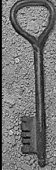
## Stream Cipher Integrity

- ◆ 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.

- ◆ This can be protected against by the careful addition of appropriate redundancy.

January 15, 2002 Practical Aspects of Modern Cryptography




## 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.

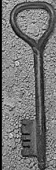
January 15, 2002 Practical Aspects of Modern Cryptography



## 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 15, 2002 Practical Aspects of Modern Cryptography

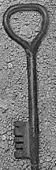


## One-Way Hash Functions

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  $H(x) = H(x')$ .

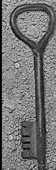
January 15, 2002 Practical Aspects of Modern Cryptography



## One-Way Hash Functions

- ◆ When using a stream cipher, a 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 15, 2002 Practical Aspects of Modern Cryptography



## A Cryptographic Hash: SHA-1

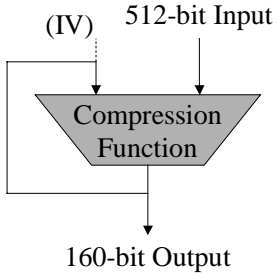
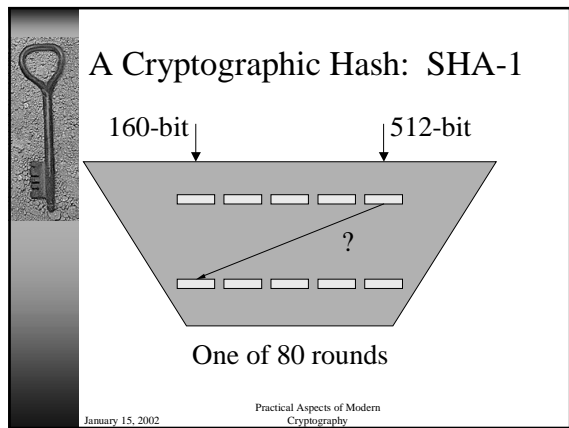
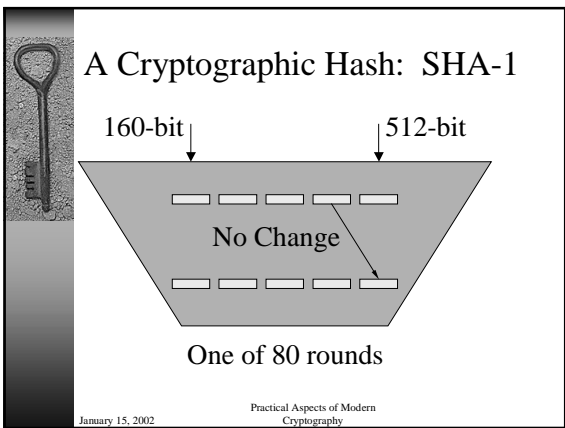
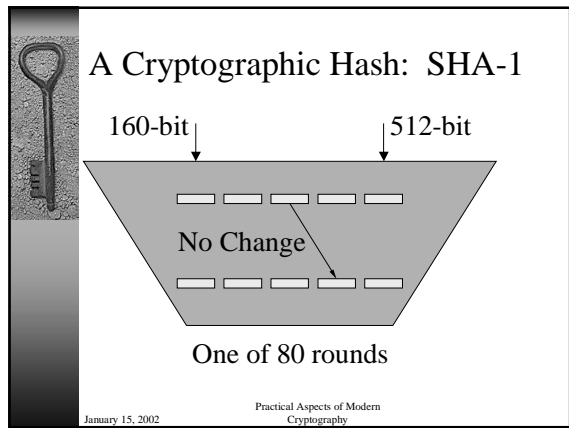
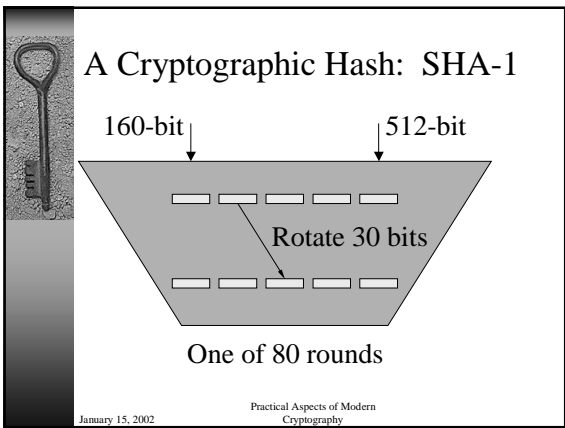
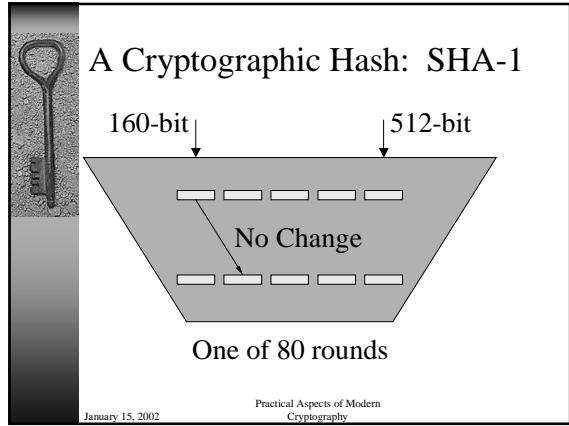
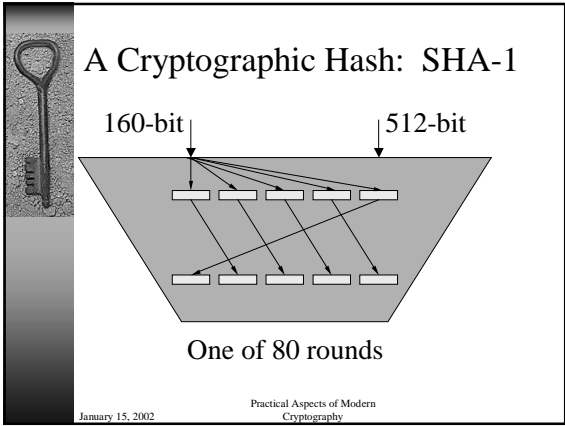


Diagram illustrating the SHA-1 compression function: A 512-bit Input (IV) is processed by a Compression Function, resulting in a 160-bit Output. The output is fed back into the input of the next iteration.

January 15, 2002 Practical Aspects of Modern Cryptography



## 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 15, 2002 Practical Aspects of Modern Cryptography

## A Cryptographic Hash: SHA-1

160-bit      512-bit

One of 80 rounds

January 15, 2002 Practical Aspects of Modern Cryptography

## 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 15, 2002 Practical Aspects of Modern Cryptography

## 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 15, 2002 Practical Aspects of Modern Cryptography

## 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 15, 2002 Practical Aspects of Modern Cryptography

## A Cryptographic Hash: SHA-1

What's in the final 32-bit transform?

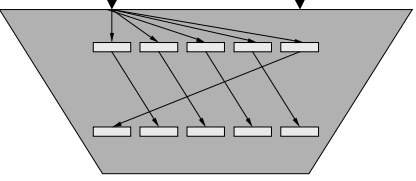
- ◆ Take the rightmost word.
- ◆ Add in the leftmost word rotated 5 bits.
- ◆ Add in a round-dependent function  $f$  of the middle three words.
- ◆ Add in a round-dependent constant.
- ◆ Add in a portion of the 512-bit message.

January 15, 2002 Practical Aspects of Modern Cryptography



## A Cryptographic Hash: SHA-1


160-bit                      512-bit



One of 80 rounds

January 15, 2002                      Practical Aspects of Modern  
Cryptography

The diagram illustrates a single round of the SHA-1 algorithm. It shows a large trapezoidal shape representing the input stream, with a 512-bit input at the top. This input is processed into four smaller rectangular blocks, each representing a 160-bit output. Arrows indicate the flow of data from the input to the four outputs. The text 'One of 80 rounds' is centered below the diagram.



## Cryptographic Tools

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

January 15, 2002                      Practical Aspects of Modern  
Cryptography

A list of cryptographic tools is presented on the right side of the slide. The tools are: One-Way Trapdoor Functions, Public-Key Encryption Schemes, One-Way Functions, One-Way Hash Functions, Pseudo-Random Number-Generators, Secret-Key Encryption Schemes, and Digital Signature Schemes. A horizontal line is drawn under the 'One-Way Functions' item.