How cryptography is used to secure web services

Josh Benaloh
Cryptographer
Microsoft Research

Transfer of Confidential Data

You (client) **Merchant (server)**

I want to make a purchase. →

← What is your Credit Card Number?

My Credit Card is 6543 2345 6789 8765. →

Transfer of Confidential Data

- But the Internet provides no privacy.
- Is there any way to protect my data from prying eyes at intermediate nodes?

Symmetric Encryption

- If the user has a pre-existing relationship with the merchant, they may have a shared secret key K – known only to the two parties.
- User encrypts private data with key K.
- Merchant decrypts data with key K.

Asymmetric Encryption

- What if the user and merchant have no prior relationship?
- Asymmetric encryption allows me to encrypt a message for a recipient without knowledge of the recipient's decryption key.

The Fundamental Equation

$$E= mc^2$$

The Fundamental Equation

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

The Fundamental Equation

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

When Z is unknown, it can be efficiently computed.

The Fundamental Equation

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

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

The Fundamental Equation

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

When Y is unknown, the problem is known as *discrete root finding* and is generally believed to be hard to solve … without the factorization of N.

The Fundamental Equation

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

The problem is not well-studied for the case when N is unknown.

How to compute $Y^X \bmod N$

Compute Y^X and then reduce mod N.

- If X, Y, and N each are 1,000-bit integers, Y^X consists of $\sim 2^{1010}$ bits.
- Since there are roughly 2^{250} particles in the universe, storage is a problem.

How to compute Y^X mod N

- Repeatedly multiplying by Y (followed each time by a reduction modulo N) X times solves the storage problem.
- However, we would need to perform $\sim 2^{900}$ 32-bit multiplications per second to complete the computation before the sun burns out.

May 17, 2005 13

How to compute Y^X mod N

Multiplication by Repeated Doubling

To compute $X \cdot Y$,

compute $Y, 2Y, 4Y, 8Y, 16Y, \ldots$

and sum up those values dictated by the binary representation of X.

Example: $26Y = 2Y + 8Y + 16Y$.

May 17, 2005 14

How to compute Y^X mod N

Exponentiation by Repeated Squaring

To compute Y^X,

compute $Y, Y^2, Y^4, Y^8, Y^{16}, \ldots$

and multiply those values dictated by the binary representation of X.

Example: $Y^{26} = Y^2 \cdot Y^8 \cdot Y^{16}$.

May 17, 2005 15

How to compute Y^X mod N

We can now perform a 1,000-bit modular exponentiation using ~1,500 1,000-bit modular multiplications.

- 1,000 squarings: $y, y^2, y^4, \ldots, y^{2^{1000}}$
- ~500 "ordinary" multiplications

May 17, 2005 16

The Fundamental Equation

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

When Y is unknown, the problem is known as *discrete root finding* and is generally believed to be hard to solve … **without the factorization of N**.

May 17, 2005 17

RSA Encryption/Decryption

- Select two large primes p and q.
- Publish the product $N = pq$.
- The exponent X is typically fixed at 65537.
- Encrypt message Y as $E(Y) = Y^X \bmod N$.
- Decrypt ciphertext Z as $D(Z) = Z^{1/X} \bmod N$.
- Note $D(E(Y)) = (Y^X)^{1/X} \bmod N = Y$.

May 17, 2005 18

RSA Signatures and Verification

- Not only is $D(E(Y)) = (Y^X)^{1/X} \bmod N = Y$, but also $E(D(Y)) = (Y^{1/X})^X \bmod N = Y$.
- To form a signature of message Y, create $S = D(Y) = Y^{1/X} \bmod N$.
- To verify the signature, check that $E(S) = S^X \bmod N$ matches Y.

May 17, 2005 19

Transfer of Confidential Data

You (client) Merchant (server)

I want to make a purchase. →

← What is your Credit Card Number?

My Credit Card is 6543 2345 6789 8765. →

May 17, 2005 20

Transfer of Confidential Data

You (client) Merchant (server)

I want to make a purchase. →

← Here is my RSA public key E.

My Credit Card is E(6543 2345 6789 8765). →

May 17, 2005 21

Intermediary Attack

You (client) Intermediary Merchant (server)

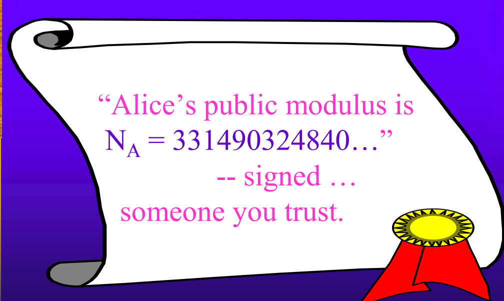
I want to make a purchase. → I want to make a purchase. →

← My public key is Ẽ. ← My public key is E.

Ẽ(CC#) → E(CC#) →

May 17, 2005 22

Digital Certificates



May 17, 2005 23

Transfer of Confidential Data

You (client) Merchant (server)

I want to make a purchase. →

← Here is my RSA public key E *and* a cert.

My Credit Card is E(6543 2345 6789 8765). →

May 17, 2005 24

Replay Attack

You (client) — Merchant (server)

I want to make a purchase. →

← Here is my RSA public key E *and* a cert.

My Credit Card is E(6543 2345 6789 8765). →

Later …

Eavesdropper — Merchant (server)

I want to make a different purchase. →

← Here is my RSA public key E *and* a cert.

My Credit Card is E(6543 2345 6789 8765). →

May 17, 2005 25

Transfer of Confidential Data

You (client) — Merchant (server)

I want to make a purchase. →

← Here is my RSA public key E *and* a cert *and* a "nonce".

My Credit Card and your nonce are E("6543 2345 6789 8765", nonce). →

May 17, 2005 26

SSL/PCT/TLS History

- 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

May 17, 2005 27

SSL/PCT/TLS

You (client) — Merchant (server)

Let's talk securely.
Here are the protocols and ciphers I understand. →

I choose this protocol and these ciphers.
Here is my public key, a cert, a nonce, etc. ←

Using your public key, I've encrypted a random symmetric key (and your nonce). →

May 17, 2005 28

SSL/TLS

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

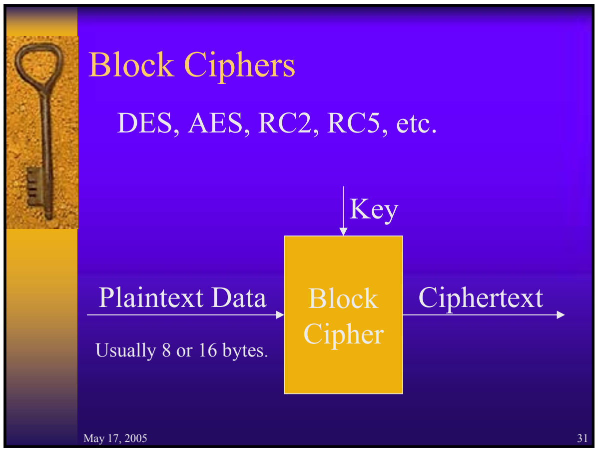
May 17, 2005 29

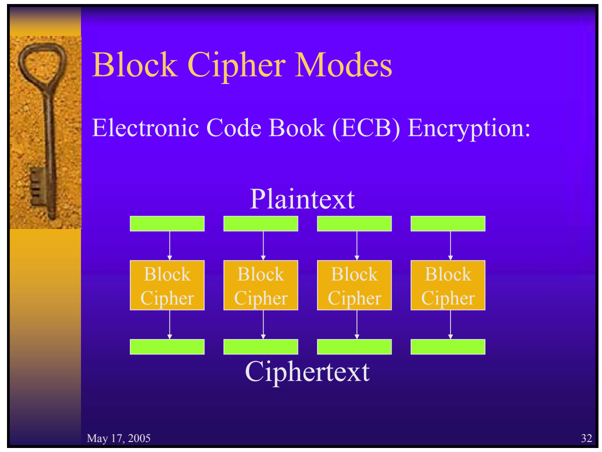
Symmetric Ciphers

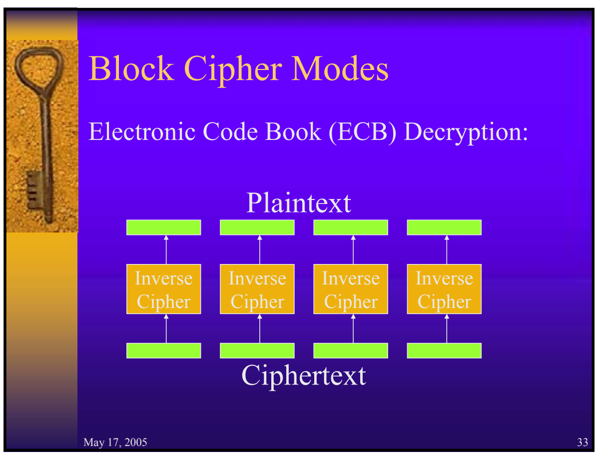
Private-key (symmetric) ciphers are usually divided into two classes.

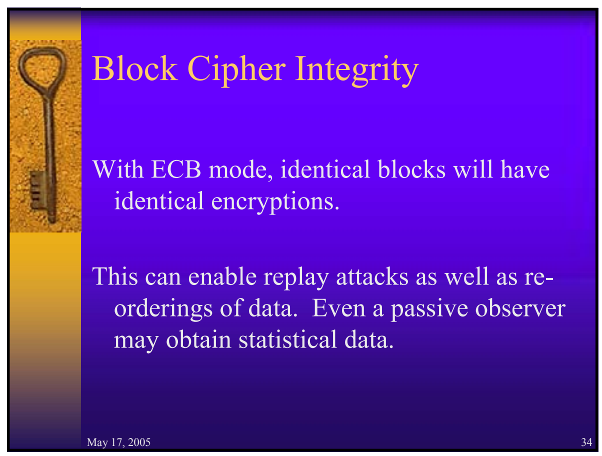
- Block ciphers
- Stream ciphers

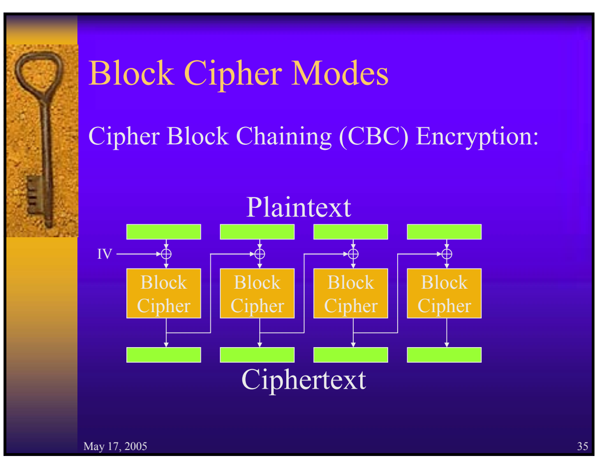
May 17, 2005 30

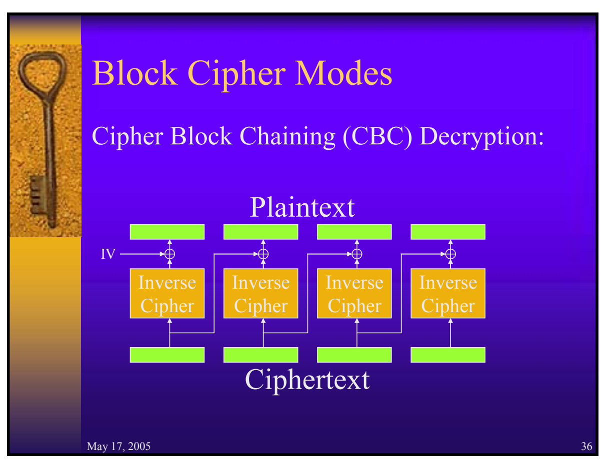

Block Ciphers
DES, AES, RC2, RC5, etc.
Key
Plaintext Data
Block Cipher
Ciphertext
Usually 8 or 16 bytes.
May 17, 2005
31


Block Cipher Modes
Electronic Code Book (ECB) Encryption:
Plaintext
Block Cipher
Block Cipher
Block Cipher
Block Cipher
Ciphertext
May 17, 2005
32


Block Cipher Modes
Electronic Code Book (ECB) Decryption:
Plaintext
Inverse Cipher
Inverse Cipher
Inverse Cipher
Inverse Cipher
Ciphertext
May 17, 2005
33


Block Cipher Integrity
With ECB mode, identical blocks will have identical encryptions.
This can enable replay attacks as well as re-orderings of data. Even a passive observer may obtain statistical data.
May 17, 2005
34


Block Cipher Modes
Cipher Block Chaining (CBC) Encryption:
Plaintext
IV
Block Cipher
Block Cipher
Block Cipher
Block Cipher
Ciphertext
May 17, 2005
35


Block Cipher Modes
Cipher Block Chaining (CBC) Decryption:
Plaintext
IV
Inverse Cipher
Inverse Cipher
Inverse Cipher
Inverse Cipher
Ciphertext
May 17, 2005
36

Stream Ciphers

RC4, SEAL, etc.

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

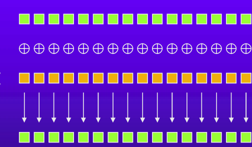
May 17, 2005 37

Stream Cipher Encryption

Plaintext:

PRNG(seed):

Ciphertext:



May 17, 2005 38

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.

May 17, 2005 39

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.

May 17, 2005 40

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.

May 17, 2005 41

One-Way Hash Functions

MD4, MD5, SHA-1, SHA-256, etc.

A *one-way hash function* is a function

$H : \{0,1\}^* \to \{0,1\}^k$ (typically k is 128 or 160)

such that, given an input value x,
one can't find $x' \neq x$ such that $H(x) = H(x')$.

May 17, 2005 42

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

May 17, 2005 43

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]

May 17, 2005 44