Foundations of Network and Computer Security

Guest Lecture for

John Black

Lecture #16

Oct 21th 2004

CSCI 6268/TLEN 5831, Fall 2004

Attack on Chess Server Methodology and Encryption Scheme

John Black

Martin Cochran

Ryan Gardner

Research Overview

- John Black, Martin Cochran, Ryan Gardner
- Summer project
- Found and analyzed several security flaws in a popular chess server
- Solutions for most problems
- No perfect solution for one!
- Wrote a paper (slashdotted)

  <http://www.cs.colorado.edu/~jrblack/papers/icc.pdf>

Presentation Outline

- Background
  - Server Background
  - Timestamping Background
- Project Overview
- Encryption
- Timestamping
- Conclusion

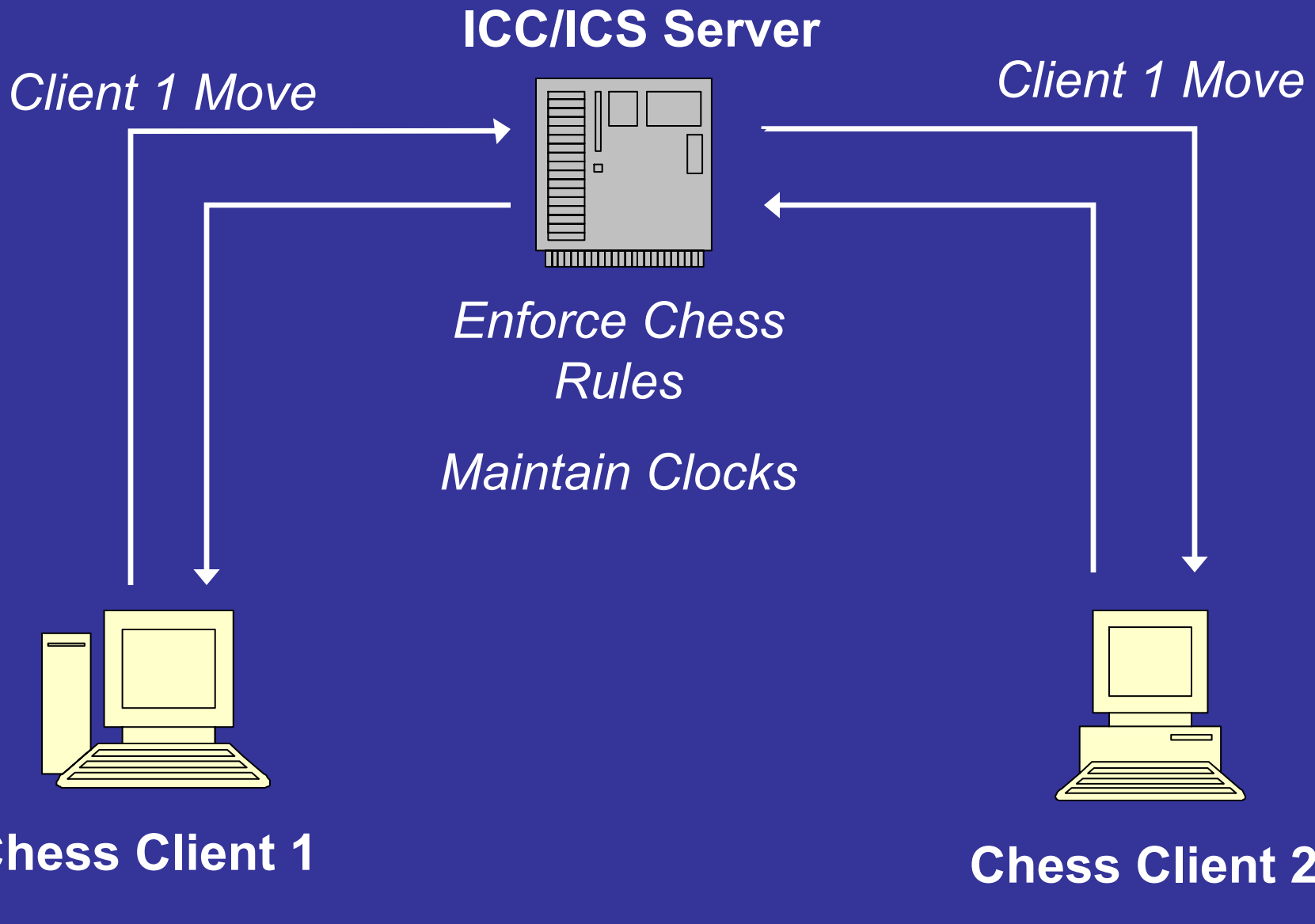
Server (ICC) Overview

- Currently ICC (Internet Chess Club)
- Over 30,000 members
- Pay Site ($60/year)
  - Students pay less
  - World's best pay nothing
- Madonna, Nicholas Cage, Will Smith, Sting, even Kasparov
- Best choice for online chess

Server History

- Was ICS (Internet Chess Server)
  - Started in early 90's
  - Free, open source
  - Basic interfaces
  - Functions
    - Clients connected to server (exclusively)
    - It sent moves in the clear
    - Maintained the state of the game
    - Maintained clocks

Basic Idea


ICC/ICS Server
Client 1 Move
Client 1 Move
Enforce Chess Rules
Maintain Clocks
Chess Client 1
Chess Client 2

Server History

- Problems
  - Server was quite buggy
  - Crashed frequently
  - Short games were unplayable
    - Network lag was deducted against the clock

Server History

- Daniel Sleator
  - Theoretical Computer Science Professor
  - Carnegie Mellon University
- Problems fixed
- Source code not released
- ICC began (no longer free)
- **Timestamping**

Timestamping Background

- Critical Issue
  - Serious chess is timed
  - Each player's clock ticks during his turn
  - Player's clock runs out, he loses
- Difficulty
  - Network lag appears as player's thinking time
- Solution
  - Timestamp each move locally at client

Timestamping Idea

Timestamping Background

- Players now send time themselves
- Can they lie?
- Sleator's solutions
  - Source code to any timestamping software is not released
  - Encrypt all data to and from server
    - (What's wrong here?)
- Further results
  - Clients used to send sensitive information

Presentation Outline

- Background
- Project Overview
- Encryption
- Timestamping
- Conclusion

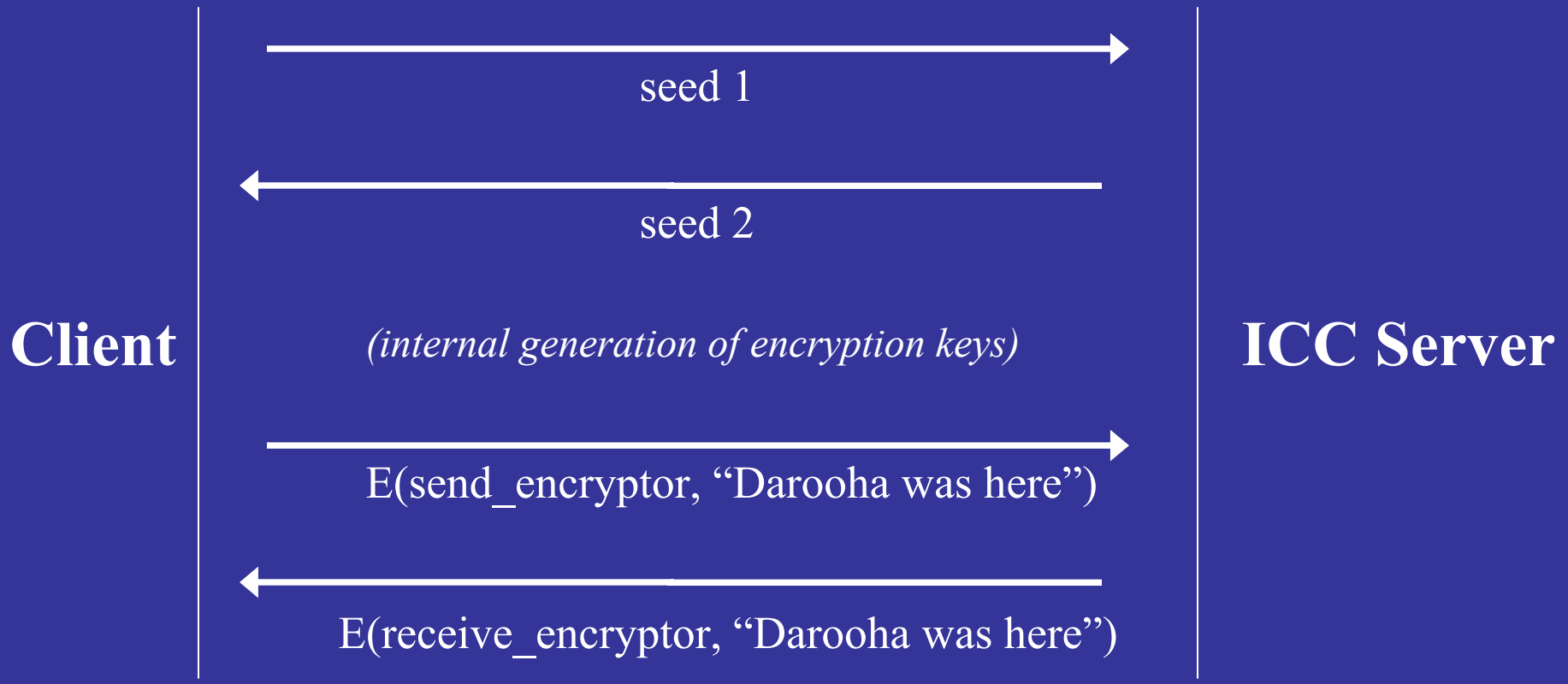
Project Overview

- Two main attacks on server
  - Encryption (three main flaws)
    - Key exchange
    - Block cipher
    - Mode of operation
  - Timestamping (cheating in chess)
- Solutions

Presentation Outline

- Background
- Project Overview
- Encryption
  - Key Exchange
  - Encryption Overview
  - Block Cipher
  - Mode of Operation
- Timestamping
- Conclusion

Encryption – Key Exchange



Encryption – Key Exchange

- Symmetric keys (seeds) exchanged in open!!!
- Only barrier
  - "Home-brewed" encryption scheme
- Response
  - Reverse engineer the linux timestamping binary
  - (Symbols not removed)

Encryption – Key Exchange

- Continuation
  - Reverse engineer additional code in Blitzin (Windows client)
- Products
  - Sniffer/decryptor
    - Linux client
    - Blitzin
  - Timestamping client
  - (not released)

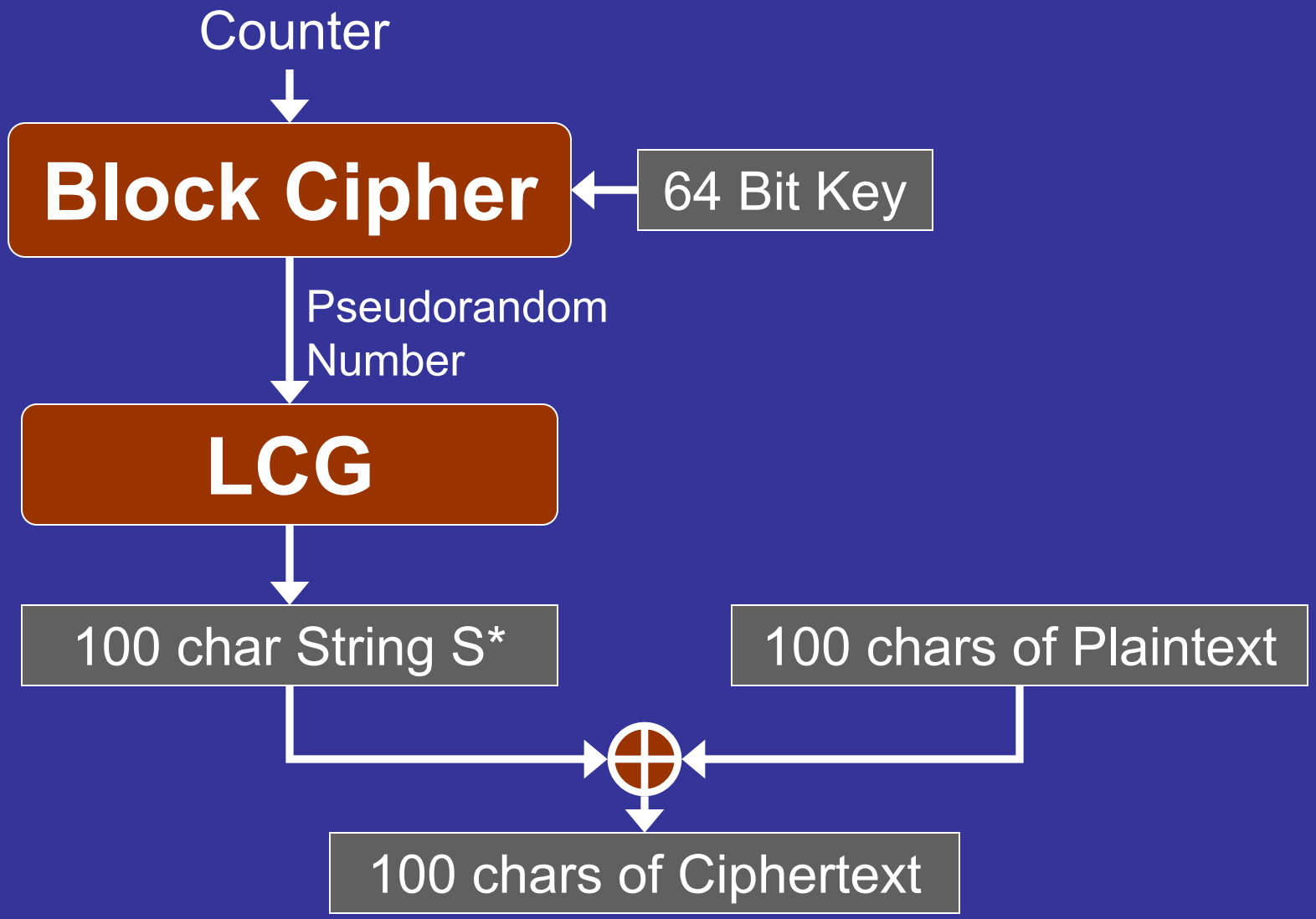
Encryption – Key Exchange

- Solution
  - Use asymmetric key exchange
    - Diffie-Hellman
    - RSA

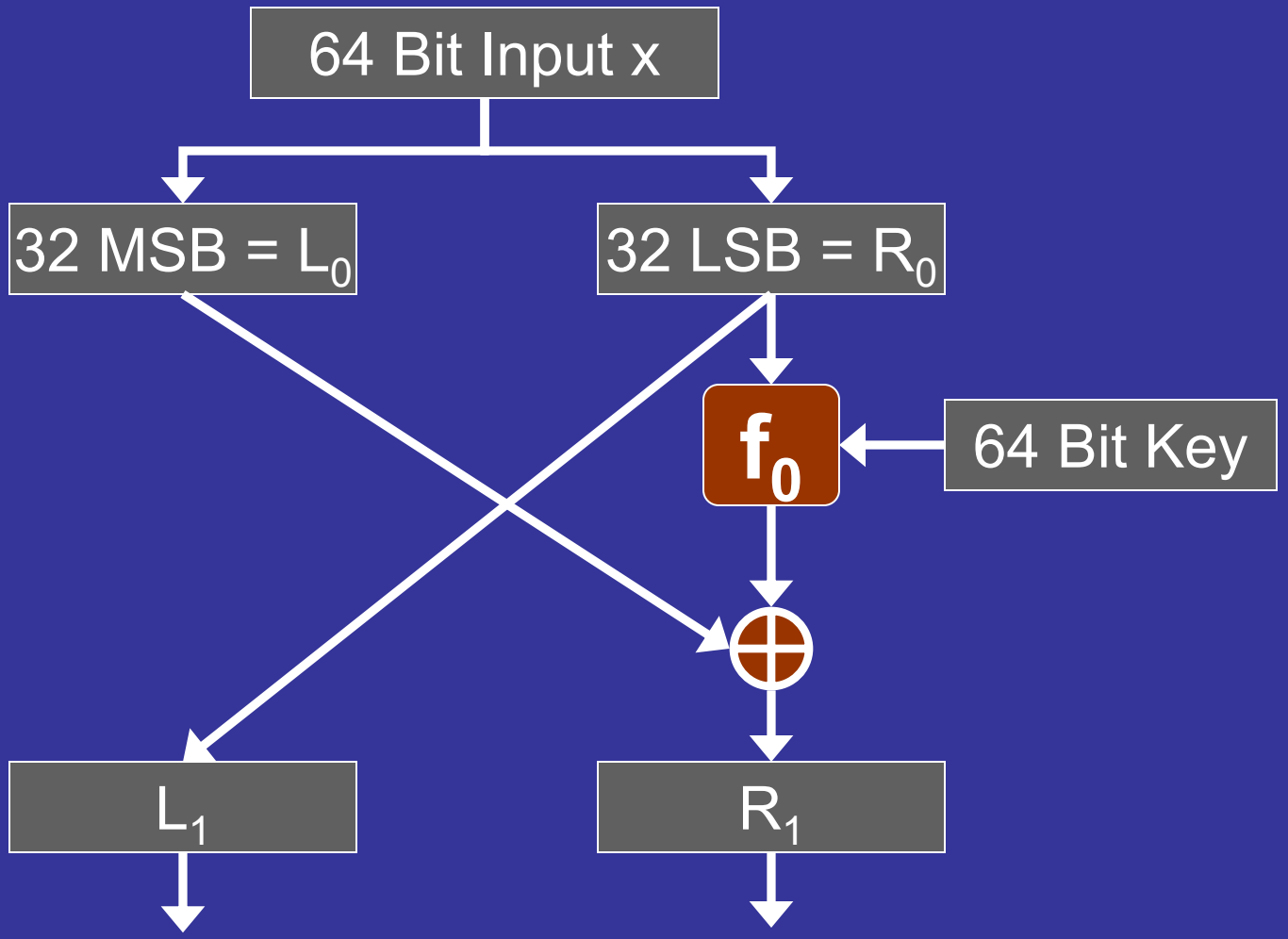
Presentation Outline

- Background
- Project Overview
- Encryption Shortcomings
  - Key Exchange
  - Encryption Overview
  - Block Cipher
  - Mode of Operation
- Timestamping Problems
- Conclusion

Encryption Overview



Encryption – Block Cipher (Feistel)



16 Rounds

The Round Function f

- $f : \{0, 1\}^{64} \times \{0, 1\}^{32} \times \{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$
- Takes 64 bit key, 32 bit input, round number
- All arithmetic is signed and modulo 2^{32}
- *stuff* is a static array of 256 32-bit values

$$f(K, V, r) = stuff\,[(V\,[0] + V\,[1] + K[r \bmod 8]) \bmod 256] + V^2$$

The Round Function f

- What's the problem here?
- Reminder: What's our goal?
  - Chosen plaintext attack on the cipher
  - (Given a black box of the cipher and a random permutation we can throw inputs at and get outputs, can we distinguish between the two?)

$$f(K, V, r) = \mathit{stuff}\,[(V[0] + V[1] + K[r \bmod 8]) \bmod 256] + V^2$$

Encryption – Block Cipher

- What happens with $V^2 \bmod 2^{32}$?
- Recall: the first bit of a 2's complement number can be thought of as having negative weight while the rest always have positive weight

$V^2 \equiv V^2 \pmod{2^{32}}$ (duh)

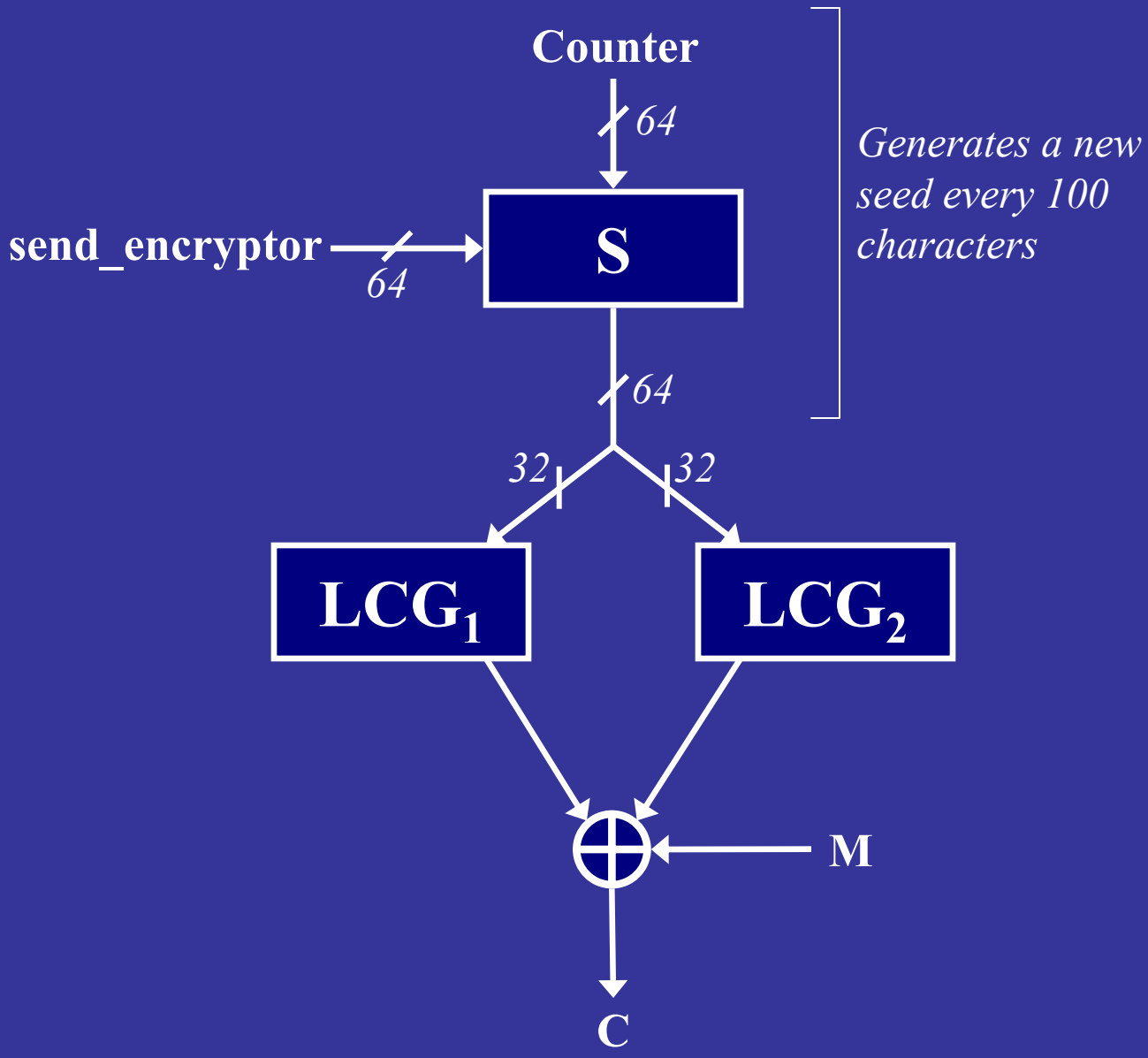
$(V - 2^{32})^2 \equiv V^2 - 2^{33}V + 2^{64} \equiv V^2 \pmod{2^{32}}$

Encryption – Block Cipher

- `f()` does not use the highest bit of input!
  - Changing bit 31 or 63 of input changes only bit 31 or 63 of output (respectively)
- Bad!
  - Identify Sleator's cipher
  - Cipher used as random number generator
  - (However, actually less practical in this case)

Presentation Outline

- Background
- Project Overview
- Encryption
  - Key Exchange
  - Encryption Overview
  - Block Cipher
  - Mode of Operation
- Timestamping
- Conclusion


Counter
64
send_encryptor
64
S
64
32
32
LCG1
LCG2
M
C
Generates a new seed every 100 characters

Encryption – Mode of Operation

- LCGs (Linear Congruential Generator)

$$x_{n+1} = 3 * x_n \pmod{43060573} + 1$$

$$y_{n+1} = 17 * y_n \pmod{2413871}$$

$$S^*_n = x_n \oplus y_n \quad \textit{(bytes)}$$

Encryption – Mode of Operation

- Poor choice of moduli
  - (We assume this mode of operation is bad anyway)
- Attack
  - Assumes knowledge of first 10 plaintext characters
  - Decrypt all 100 in block
  - <2 seconds on test program

Encryption – Mode of Operation

- Attack overview
  - Try to guess y_i outright (only 2413871 possible values)
  - Then we can determine lower bytes of the corresponding x_i's
  - By examining the ten values we have we can (almost always) determine proper x_i's if we have found the correct y_i (not going into the details of this)

Encryption - Conclusions

- Two researched problems
  - Block cipher
  - Mode of operation
- Solution
  - Proven authenticated encryption scheme
    - (OCB, IAMP, EAX)

Presentation Outline

- Background
- Project Overview
- Encryption
- Timestamping
  - Recap
  - Problems
- Conclusion

Timestamping Recap

- Concerns
  - With local timestamping of moves can people cheat?
- Sleator's solutions
  - Control source code
  - Encrypt
- Problems
  - Reverse engineer binary
    - Write own fake timestamp client
    - Just hack the binary of existing code
  - (Other problems, mention later)

Timestamping

- Additional measures
  - Strip symbols
  - Obfuscate code
- No perfect solution
  - Specialty hardware
  - Remove timestamping ability (horrible)
  - Estimate lag to host from server
  - Estimate lag to some number of hops
  - Send a Java program for each game with a unique key embedded in it

Timestamping

- Other Problems
  - Must determine time at some point
  - Requires operating system call!
  - Easy to hack
- Ideas?
  - Talk to John

Presentation Outline

- Background
- Project Overview
- Encryption
- Timestamping
- Conclusion

Conclusion

- Designing cryptosystems
  - Very difficult
  - Wagner quote
- Timestamping security model
  - Formidable
  - Similar to DRM
  - No solutions, still existing problem

Wagner Quote

Well known professor from Berkeley –

> "What makes you think you can invent a good cipher if you have no expertise in the subject? Maybe you can, but it's not terribly likely. Imagine how you would react if your doctor told you "You have appendicitis, a disease that is life-threatening if not treated. We have a time-tested cure that cures 99% of all patients with no noticeable side-effects, but I'm not going to give you that: I'm going to give you a new experimental treatment my cousin dreamed up last week. No, my cousin has no medical training. No, I have no evidence that the new treatment will work, and it's never been tested or analyzed in depth -- but I'm going to give it to you anyway because my cousin thinks it is good stuff." You'd find another doctor, I hope. Rational people leave medical care to the medical experts. The medical experts have a much better track record than the quacks."
>
> -- David Wagner PhD, sci.crypt, 19th Oct 02

Ethics

- Paper release
  - To Dan Sleator first
  - Gave him time
- No source code released

Questions?