CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

Admin

- Lab 4 Part B feedback will go out by Thursday at the latest
  - Start your patch before then. Really.
  - Extra Credit submissions are up!

- Final exam review Thursday section

- Fill out the form (see Ed/email) for left-hand desk and other seating requests.

- Course feedback is now open, please fill it out!
  - https://uw.iasystem.org/survey/309432

Exceptional Access

Or, letting the government into locked devices

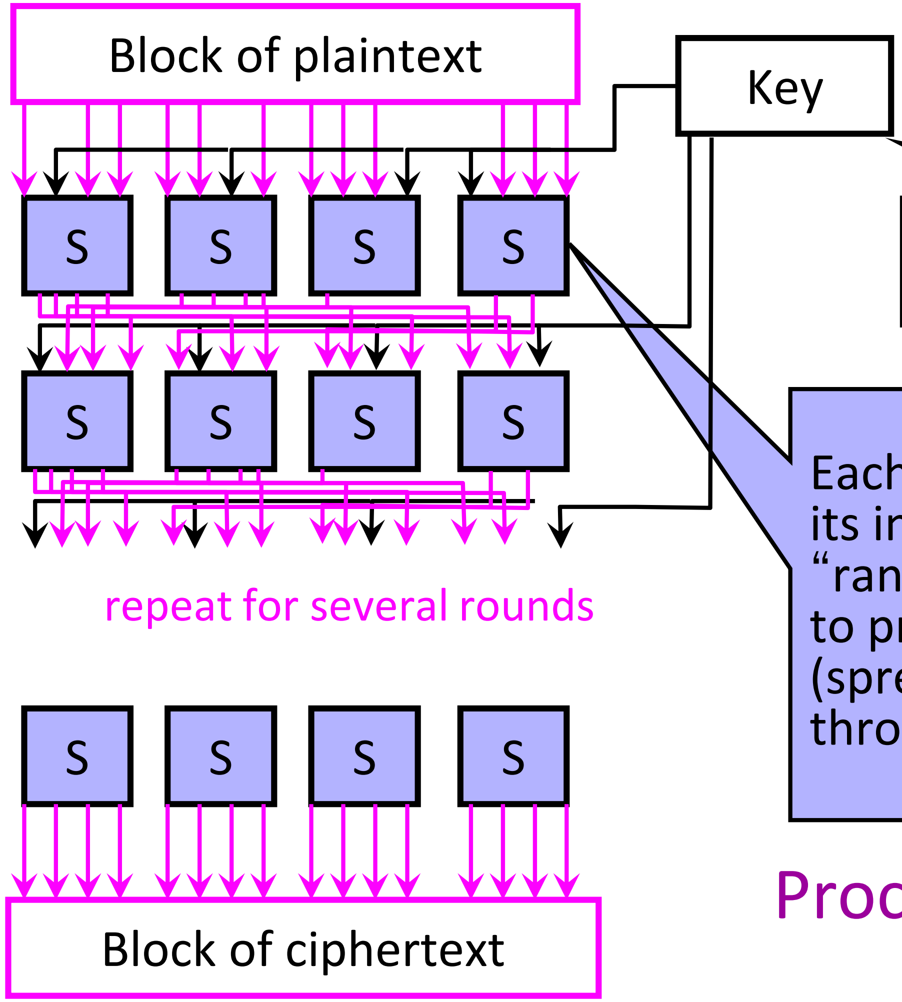
A brief aside, useful for consideration

- DES S-boxes

- Dual_EC_DRBG

DES S-boxes standardization

- Recall:

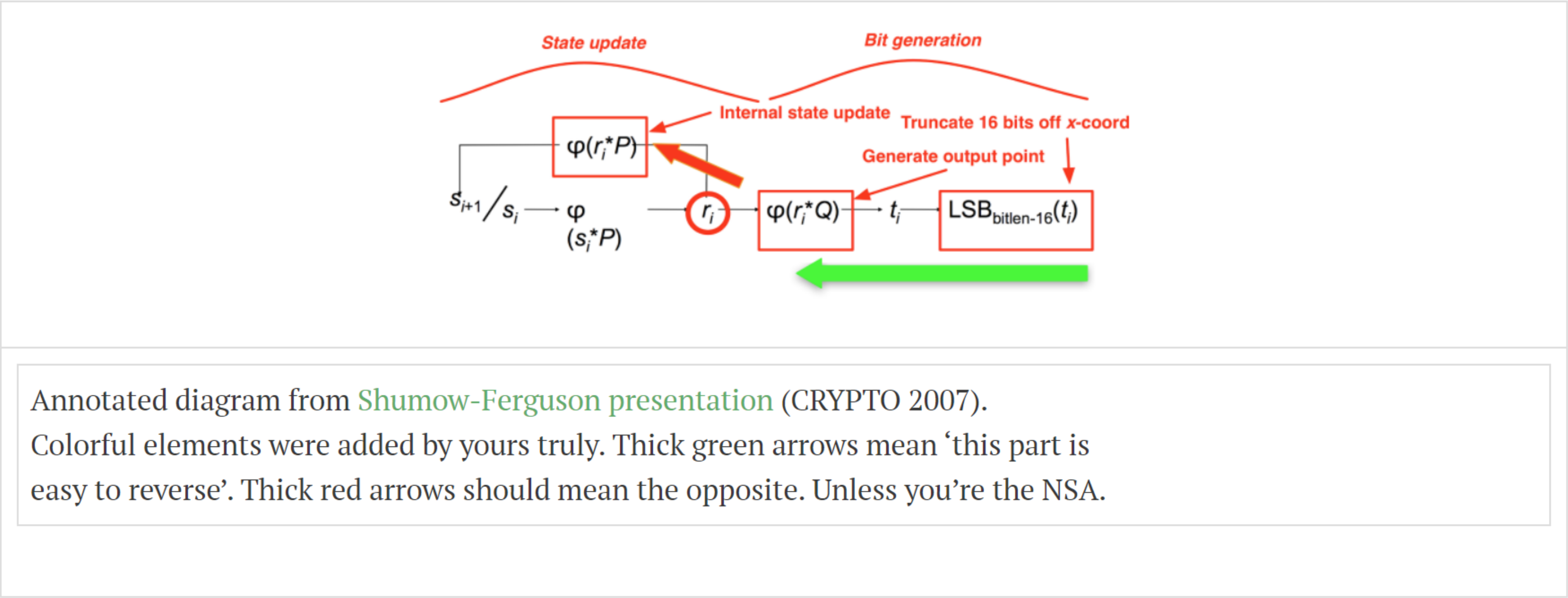


Add some secret key bits to provide confusion

Each S-box transforms its input bits in a "random-looking" way to provide diffusion (spread plaintext bits throughout ciphertext)

Procedure must be reversible (for decryption)

DUAL_EC_DRBG



Annotated diagram from Shumow-Ferguson presentation (CRYPTO 2007). Colorful elements were added by yours truly. Thick green arrows mean ‘this part is easy to reverse’. Thick red arrows should mean the opposite. Unless you’re the NSA.

https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/

https://hovav.net/ucsd/dist/juniper.pdf

DUAL_EC_DRBG – Is it really a backdoor?

- Cannot recommend enough: https://securitycryptographywhatever.com/2024/12/07/dual-ec-drbg/

- Justin Schuh argues well that this was not a backdoor.
  - (Former NSA, former Google Chrome.)

History: Dual-use

- Technologies under restriction regimes may be *dual-use*

- A missile is *not* dual-use
  - Hunting firearms *are* dual-use

- That is, military and civilian applications

Dual-use

- Gradescope

History: Cryptography

- Post WWII all cryptography was a ‘munition’
    - Subject to export restrictions
    - Fundamentally a military technology

- This was (mostly) reasonable

- It stopped being (as) reasonable once electronic communications became a thing
    - Really clearly dual-use at this point

History: The crypto wars (1st)

- Cold war ends in 1991
- Some export restrictions are lifted in 1992
  - <40bits of key systems allowed
  - 40 bits is crackable in days at the time

- PGP (Pretty Good Privacy) written in 1992
  - >>>40 bits

- “Crypto wars” kick off as a reaction to restrictions

History: SSL in the 90s

- Netscape had SSL (HTTPS) for e-commerce

- Problem: SSL was 128bits of key

- Solution: Two versions of the browser
  - US Version: 128bits
  - International Version: 40bits (reveals 88bits)

History: The Clipper Chip

- 1994 a new system is proposed: Skipjack
- 80-bits of security
- “Trap-door” built in to allow government recovery of messages
  - This was public
- Proposal was to put the “clipper chip” into everything

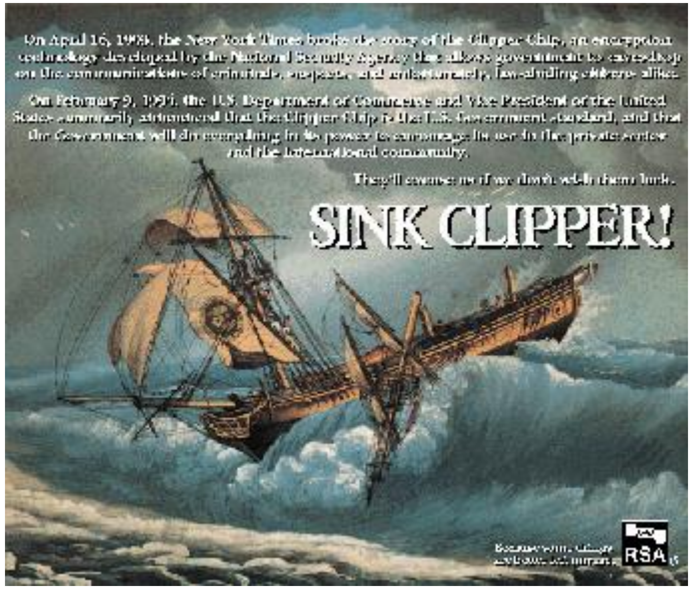
History: The Clipper Chip

- Argument was that ‘terrorists’ would be caught

- This was… not well received

- It also had a number of serious technical flaws

- It died reasonably fast



On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll come at us if we don't sink them first.

By Source (WP:NFCC#4), Fair use, https://en.wikipedia.org/w/index.php?curid=48926067

https://www.mattblaze.org/papers/escrow-acsac11.pdf

History: Crypto wars end

- In 2000 restrictions are eased
    - (Per 1996 order that made this possible)

- AES is standardized

- Cryptography ‘golden age’ starts

Today: Continuation

- Cryptography is back in the headlines

- It is trivial to have encrypted data
  - Mobile phones
  - Backup systems
  - Messaging platforms

- Governments want access to encrypted data

Good starting points

- Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion - Stefan Savage
  - http://cseweb.ucsd.edu/~savage/papers/lawful.pdf

- The Export of Cryptography in the 20th Century and the 21st - Whitfield Diffie and Susan Landau
  - https://privacyink.org/pdf/export_control.pdf

- Key Escrow from a Safe Distance Looking Back at the Clipper Chip
  - https://www.mattblaze.org/papers/escrow-acsac11.pdf