

CSE 484: Computer Security and Privacy

Encryption and Government

Spring 2024

David Kohlbrenner

dkohlbre@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Logistics

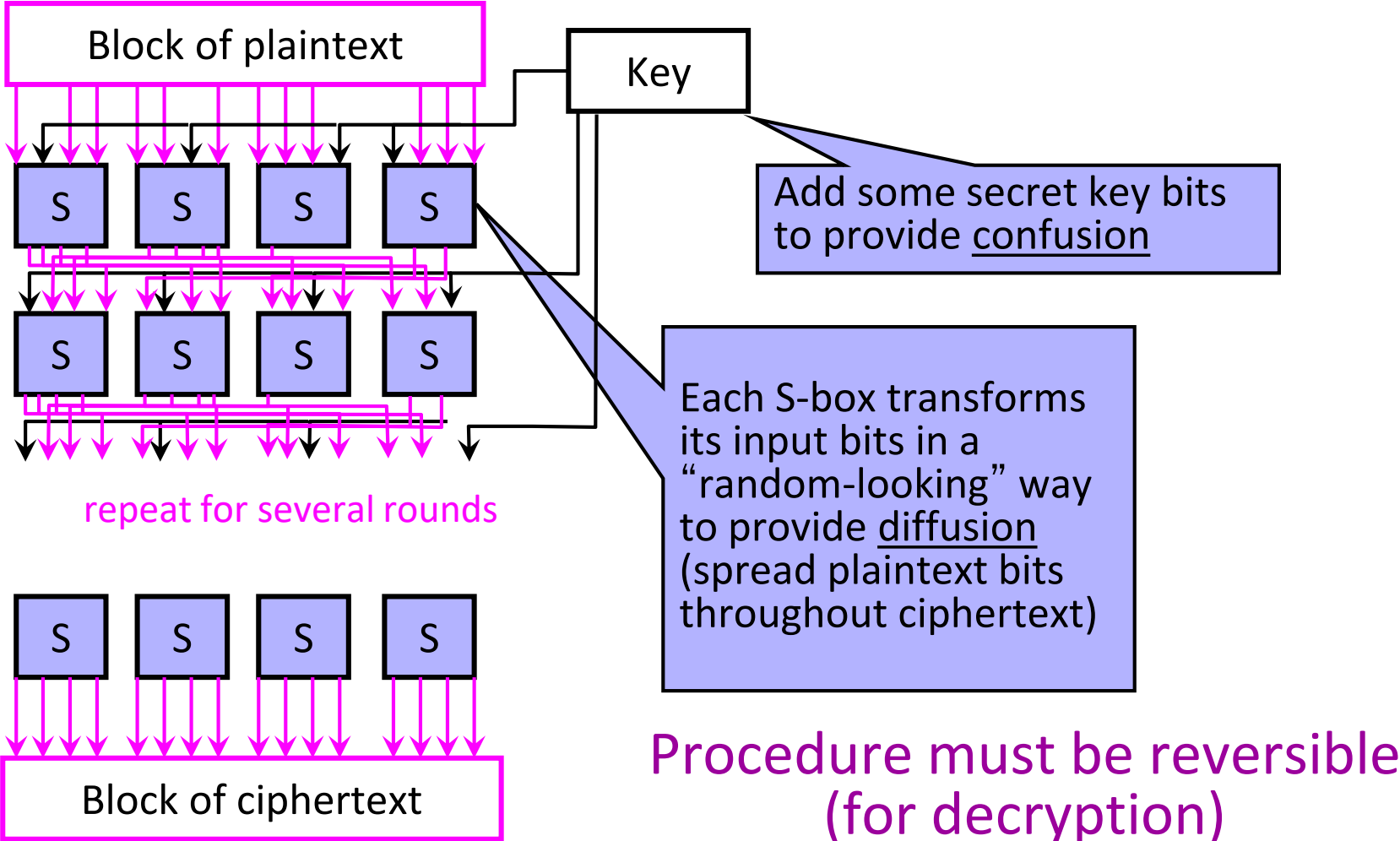
- The intro for today is recorded but discussion is not
- FP Part A grading starting, will release an example patch this weekendish
- FP part B (RCAs) due Wednesday, we'll get fast feedback to you
- Please fill out the feedback form!
 - <https://uw.iasystem.org/survey/290594>

A brief aside, useful for consideration

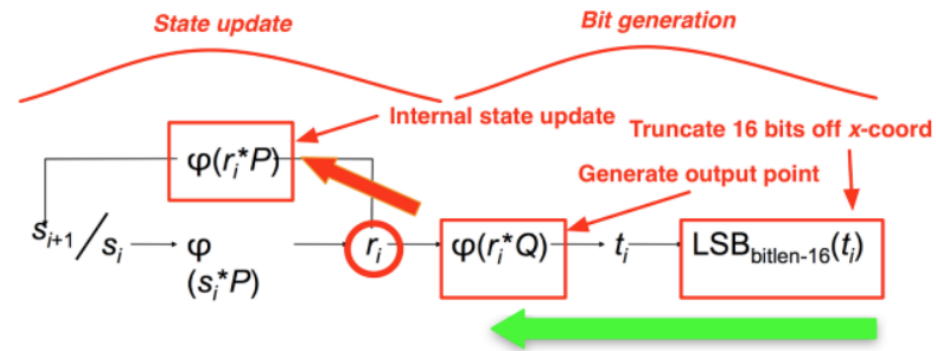
- DES S-boxes
- Dual_EC_DRBG

DES S-boxes standardization

• Recall:



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>

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

Discuss

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



By Source (WP:N FCC#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-ac sac11.pdf>