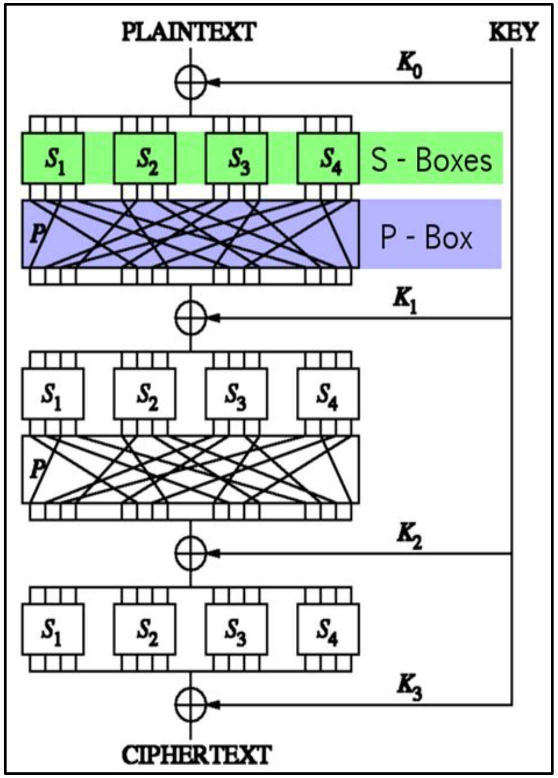
Small Box Cryptography
and
The Provable Security of SPNs

Yevgeniy Dodis

New York University



Joint work with

Jonathan Katz, John Steinberger, Aishwarya Thiruvengadam, Zhe Zhang

WHAT IS THE BIGGEST OPEN PROBLEM IN CRYPTOGRAPHY?

WHAT IS THE BIGGEST OPEN PROBLEM IN CRYPTOGRAPHY?

Of course, no right answer, but my answer is…

WHAT IS THE BIGGEST OPEN PROBLEM IN CRYPTOGRAPHY?

Of course, no right answer, but my answer is…

(Provable) Security of AES

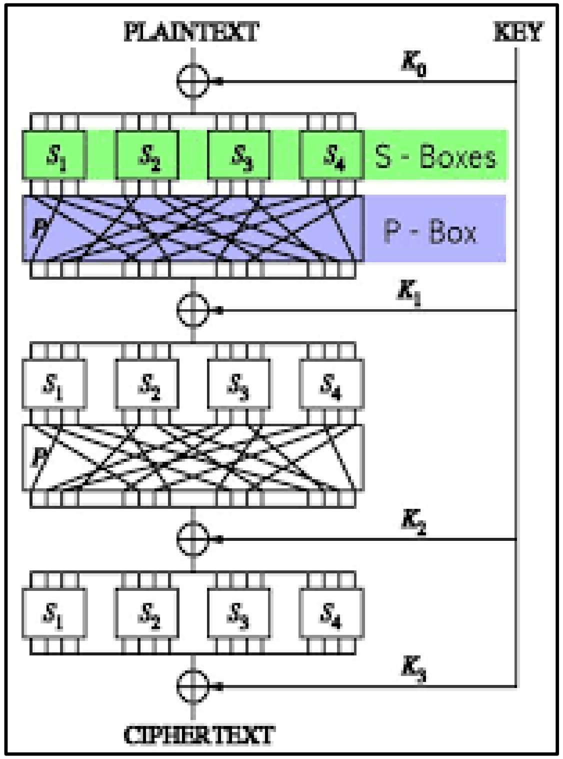
WHAT IS THE BIGGEST OPEN PROBLEM IN CRYPTOGRAPHY?

Of course, no right answer, but my answer is…

(Provable) Security of AES

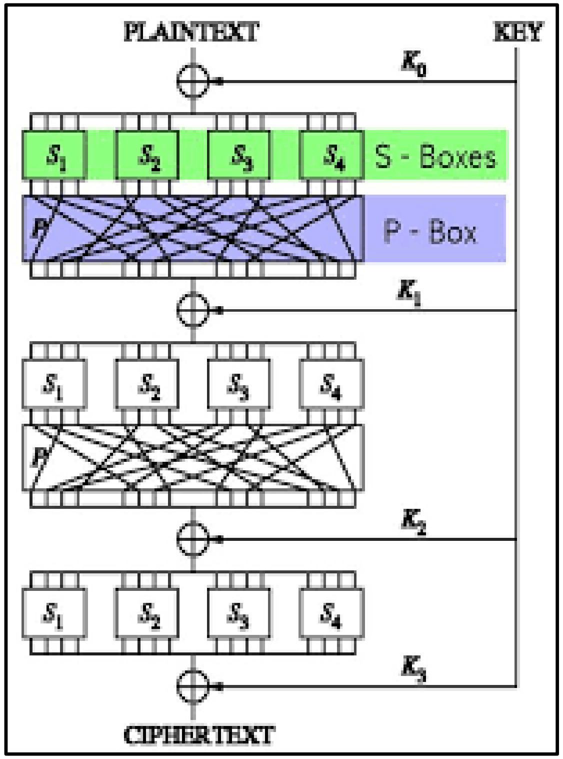
What is AES?

- Substitution-Permutation Network (SPN)



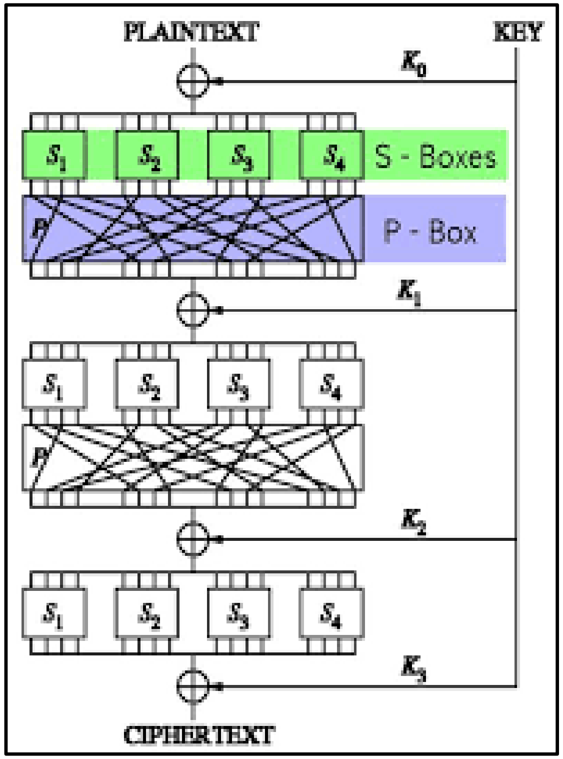
What is AES?

- Substitution-Permutation Network (SPN)
  - Several (e.g., 10) rounds of:
    - Key addition (simple XOR), governed by ad hoc "key schedule"
    - Substitution: parallel *small* S-boxes (AES case: inversion$^+$ in GF[2^8])
    - Permutation: linear *big* P-box (AES case: shift rows/columns)



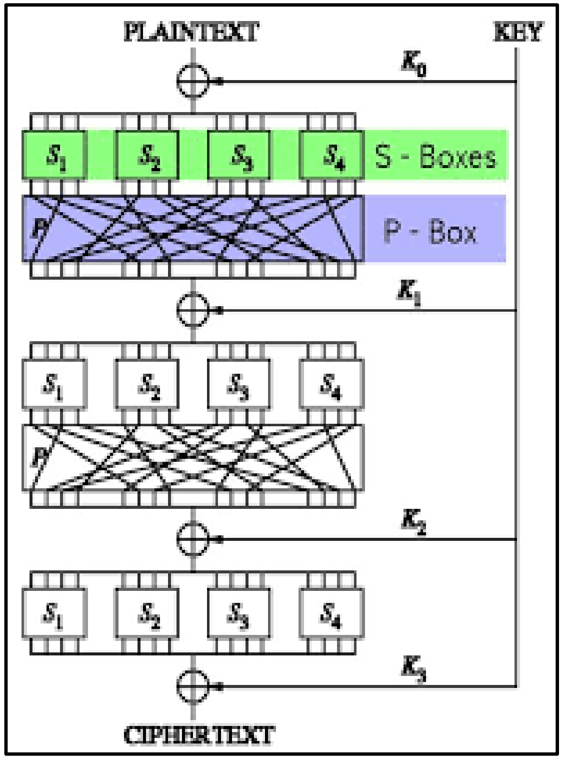
What is AES?

- Substitution-Permutation Network (SPN)
  - Several (e.g., 10) rounds of:
    - Key addition (simple XOR), governed by ad hoc “key schedule”
    - Substitution: parallel *small* S-boxes (AES case: inversion$^+$ in GF[2^8])
    - Permutation: linear *big* P-box (AES case: shift rows/columns)
- S-box: only non-linear piece



What is AES?

- Substitution-Permutation Network (SPN)
  - Several (e.g., 10) rounds of:
    - Key addition (simple XOR), governed by ad hoc "key schedule"
    - Substitution: parallel *small* S-boxes (AES case: inversion⁺ in GF[2^8])
    - Permutation: linear *big* P-box (AES case: shift rows/columns)
- S-box: only non-linear piece
- Many popular ciphers follow same design…



Can we Prove Security?

Can we Prove Security?

- Not unconditionally, without *P* vs. *NP*…
  - [MV15]: resilience to linear/differential cryptanalysis (restricted type of CPA attack)

Can we Prove Security?

- Not unconditionally, without *P* vs. *NP*…
  - [MV15]: resilience to linear/differential cryptanalysis (restricted type of CPA attack)
- Idealized Model/Assumption?
  - Unclear how: S-box is the *only source of hardness*, and it is small by design (8-32 bits)

Can we Prove Security?

- Not unconditionally, without *P* vs. *NP*…
  - [MV15]: resilience to linear/differential cryptanalysis (restricted type of CPA attack)
- Idealized Model/Assumption?
  - Unclear how: S-box is the *only source of hardness*, and it is small by design (8-32 bits)
- No sound theory of hardness from "iterating something simple/small for many rounds"
  - Until this work ☺

Small-Box Cryptography

Small-Box Cryptography

- Mixture of proofs and hardness conjectures

Small-Box Cryptography

- Mixture of proofs and hardness conjectures
    1. Traditional (hard/impressive) *reduced-round* PROOF

Small-Box Cryptography

- Mixture of proofs and hardness conjectures
  1. Traditional (hard/impressive) *reduced-round* PROOF
  2. Hardness amplification step (possibly PROVABLE)

Small-Box Cryptography

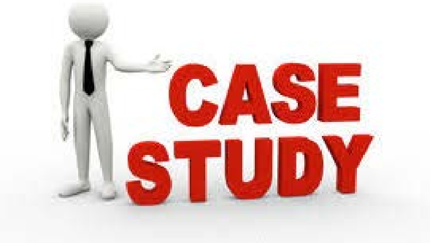
- Mixture of proofs and hardness conjectures
  1. Traditional (hard/impressive) *reduced-round* PROOF
  2. Hardness amplification step (possibly PROVABLE)
  3. Big-to-Small CONJECTURE ("OWF of Small-Box")

Small-Box Cryptography

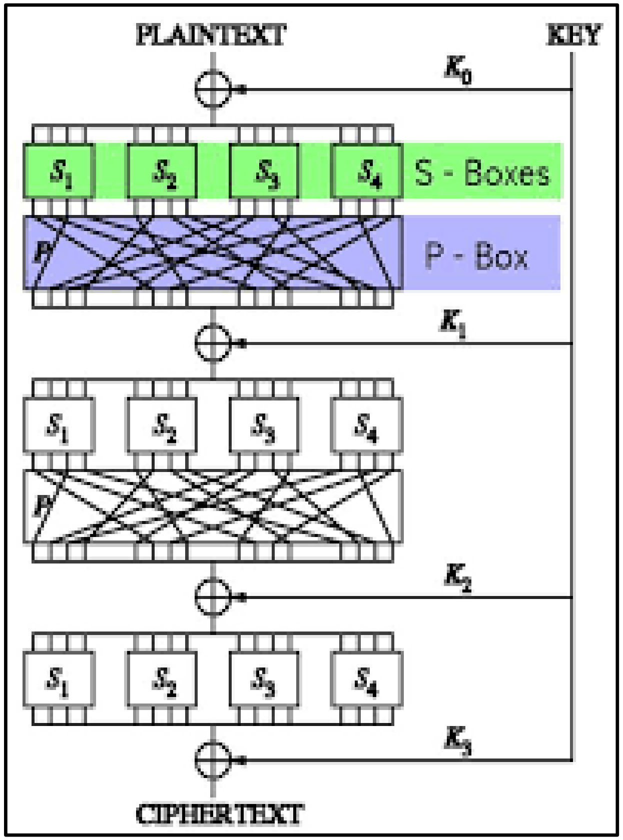
- Mixture of proofs and hardness conjectures
  1. Traditional (hard/impressive) *reduced-round* PROOF
  2. Hardness amplification step (possibly PROVABLE)
  3. Big-to-Small CONJECTURE ("OWF of Small-Box")
- Explains existing and guides new designs
  – No unspecified "big components"! (Almost) real AES!

Small-Box Cryptography

- Mixture of proofs and hardness conjectures
  1. Traditional (hard/impressive) *reduced-round* PROOF
  2. Hardness amplification step (possibly PROVABLE)
  3. Big-to-Small CONJECTURE (“OWF of Small-Box”)
- Explains existing and guides new designs
  - No unspecified “big components”! (Almost) real AES!
- Precise quantitative bounds, with explicit dependence on number of rounds
  - Strong, but *more conservative* than real-world, choices


CASE
STUDY

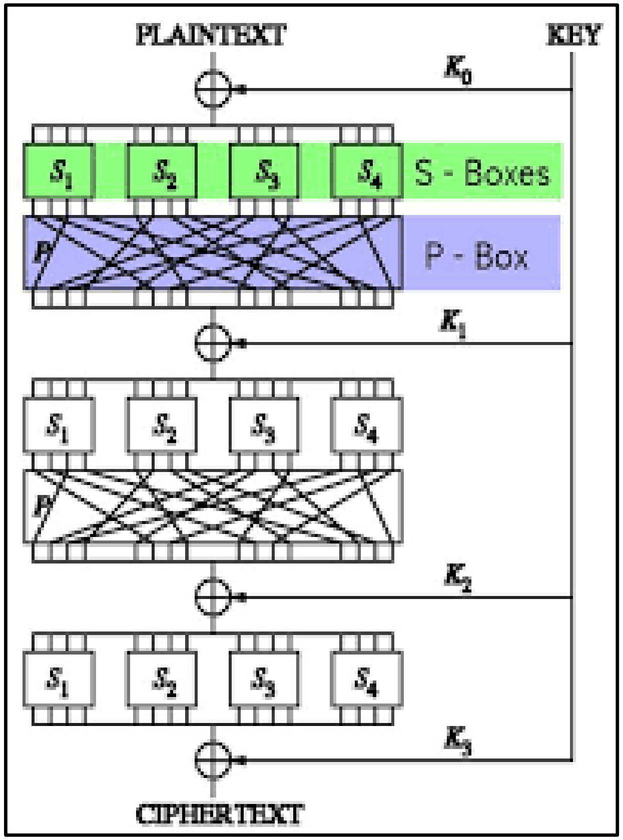
: SPNs (and AES)


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
S - Boxes
P
P - Box
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT

: SPNs (and AES)

- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}$$

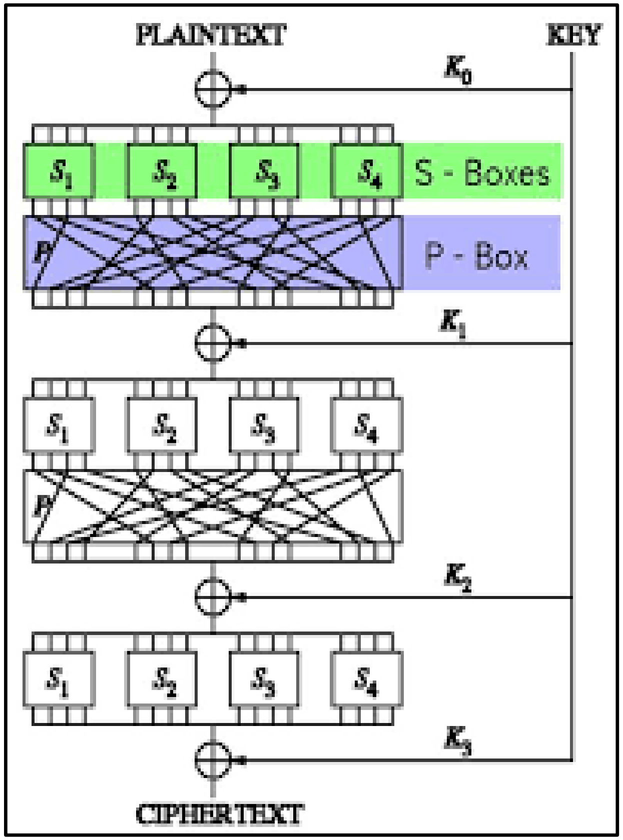


: SPNs (and AES)

- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}$$

(10^{-8} in 10 rounds AES, 2^{-64} in 24 rounds)



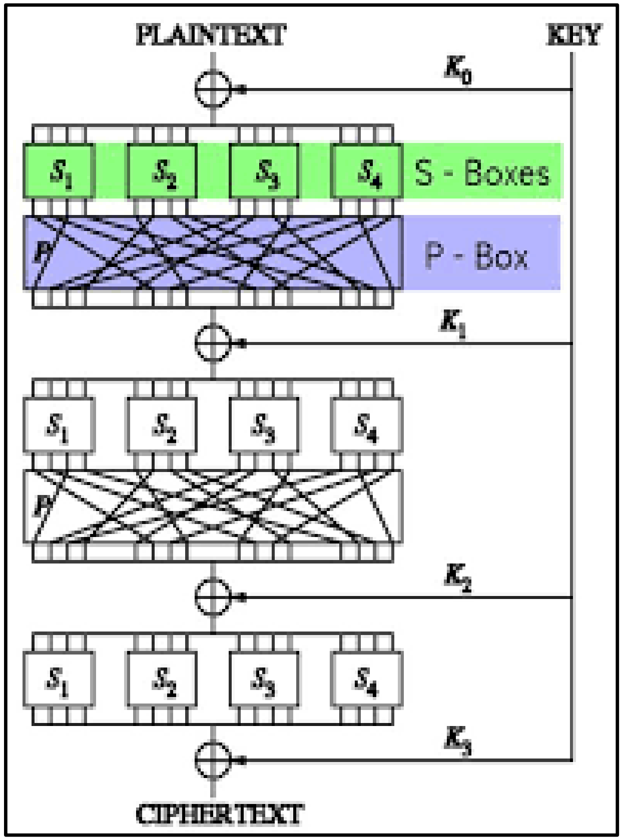
: SPNs (and AES)

- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\boxed{\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}}$$

(${10}^{-8}$ in 10 rounds AES, 2^{-64} in 24 rounds)

- With random S-boxes (can hardwire!)



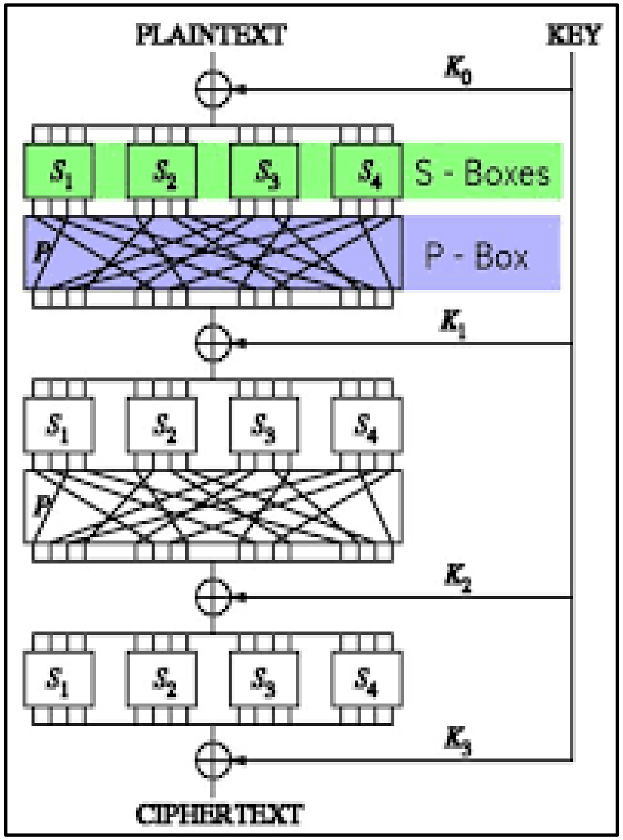
: SPNs (and AES)

- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\boxed{\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}}$$

(10^{-8} in 10 rounds AES, 2^{-64} in 24 rounds)

- With random S-boxes (can hardwire!)
- With any linear P-box whose matrix and its inverse have no 0's in GF[2^{8}]



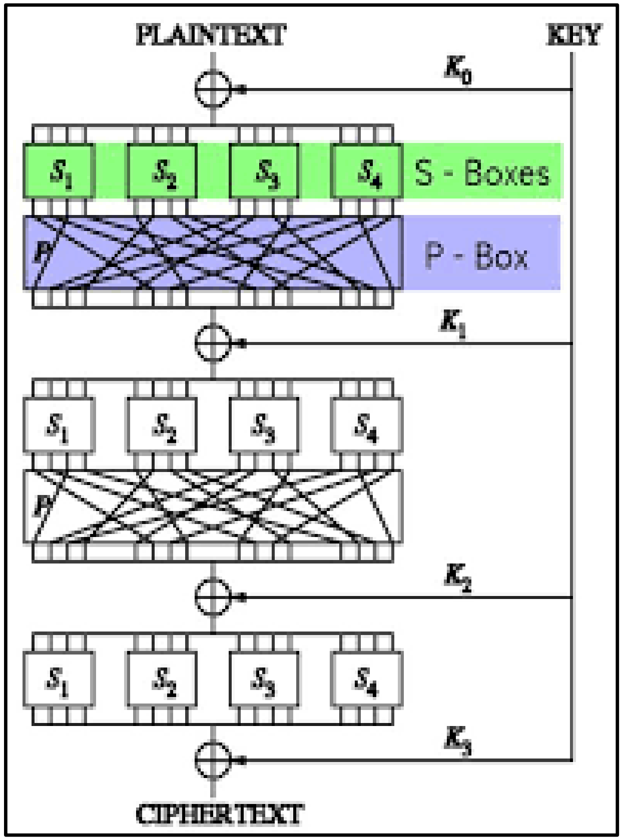
: SPNs (and AES)

- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\boxed{\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}}$$

(10^{-8} in 10 rounds AES, 2^{-64} in 24 rounds)

- With random S-boxes (can hardwire!)
- With any linear P-box whose matrix and its inverse have no 0's in GF[2^8]
- Almost real AES!



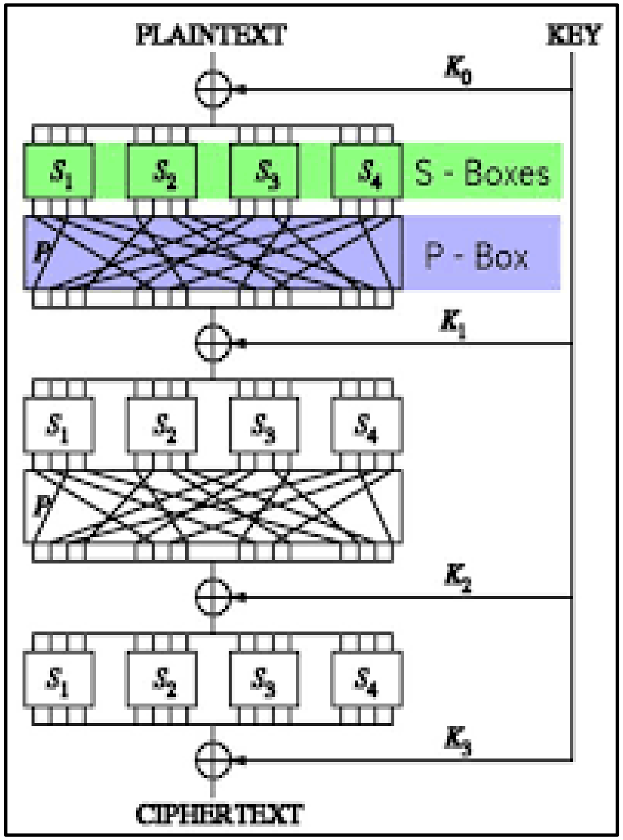
: SPNs (and AES)

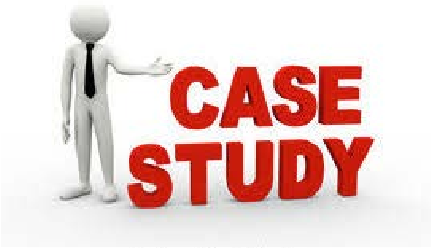
- Most aggressive security ε using 8-bit S-box (ignore time for now):

$$\boxed{\varepsilon = 2^{-8r/3} \text{ in } r \text{ rounds}}$$

(${10}^{-8}$ in 10 rounds AES, 2^{-64} in 24 rounds)

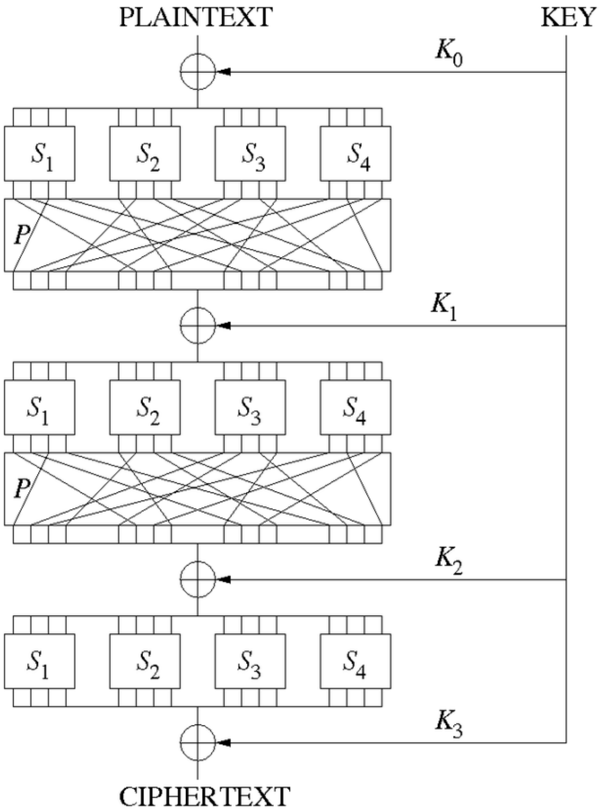
- With random S-boxes (can hardwire!)
- With any linear P-box whose matrix and its inverse have no 0's in GF[2^8]
- Almost real AES!
- Good guidance for future designs
  – Quantitative, round-dependent security
  – No unspecified components





CASE
STUDY

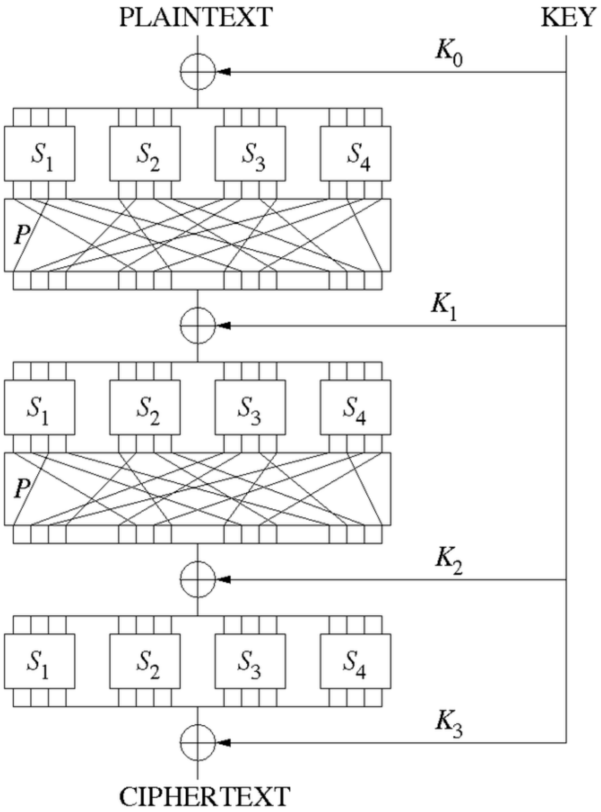
: SPNs (and AES)

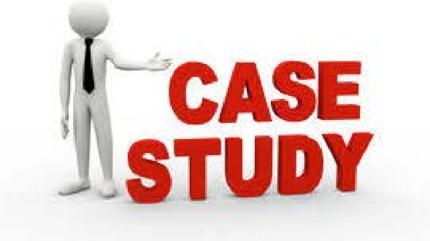


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT

: SPNs (and AES)

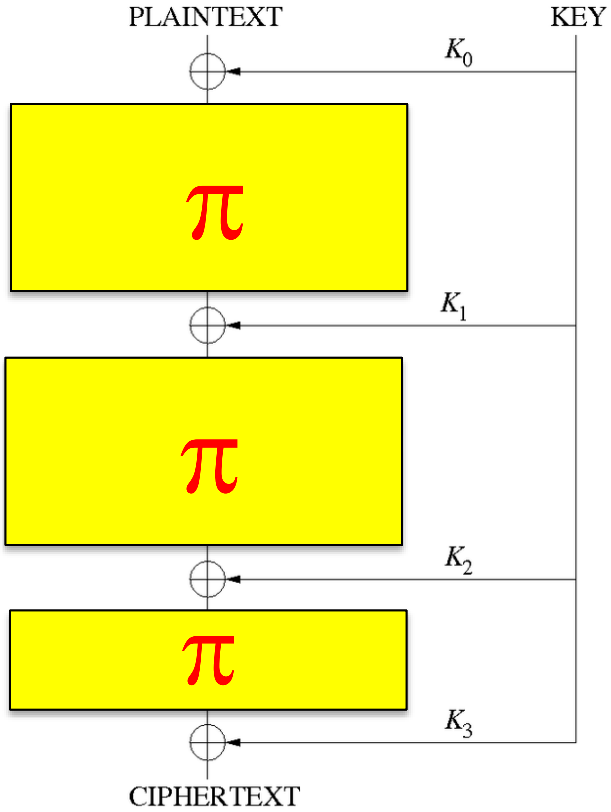
- Replace substitution-permutation structure as one big permutation π

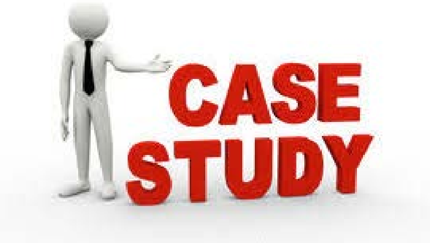




: SPNs (and AES)

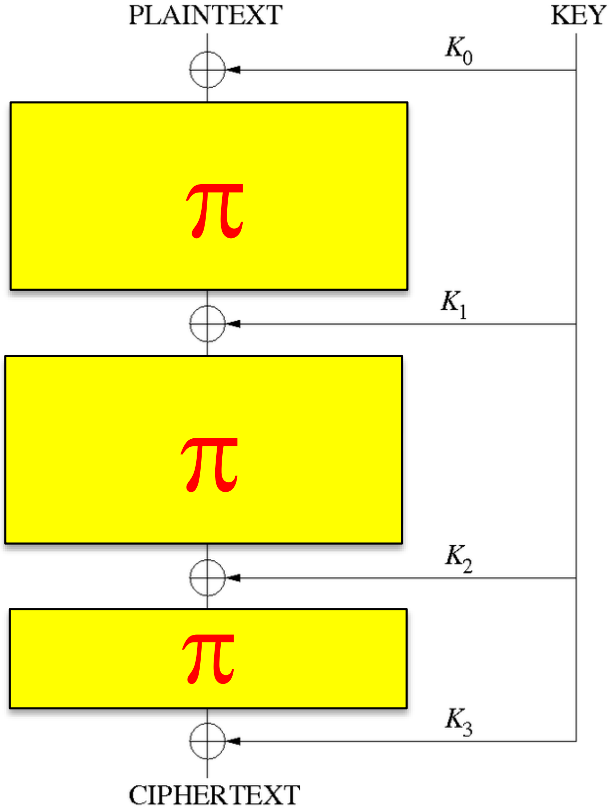
- Replace substitution-permutation structure as one big permutation π





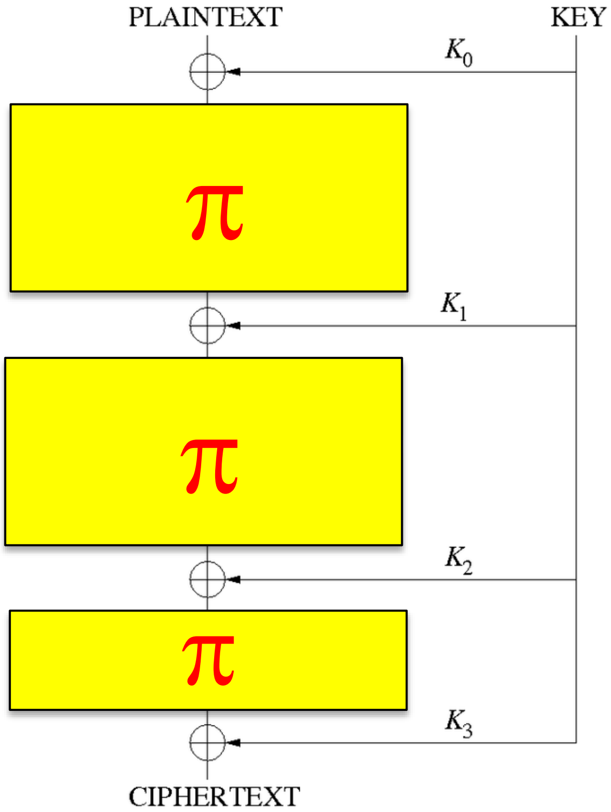
: SPNs (and AES)

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call “SPN”



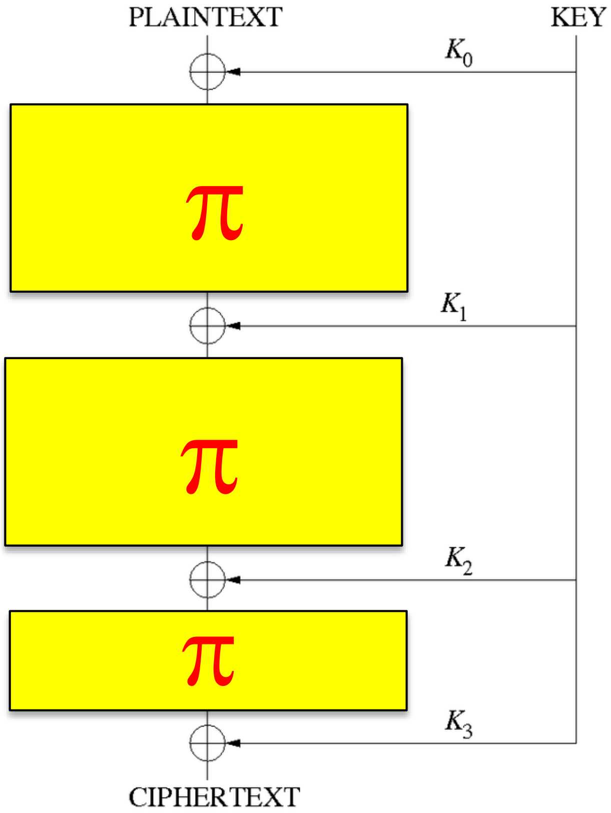
: SPNs (and AES)

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call “SPN”
  - Solution: key alternating ciphers (KAC)



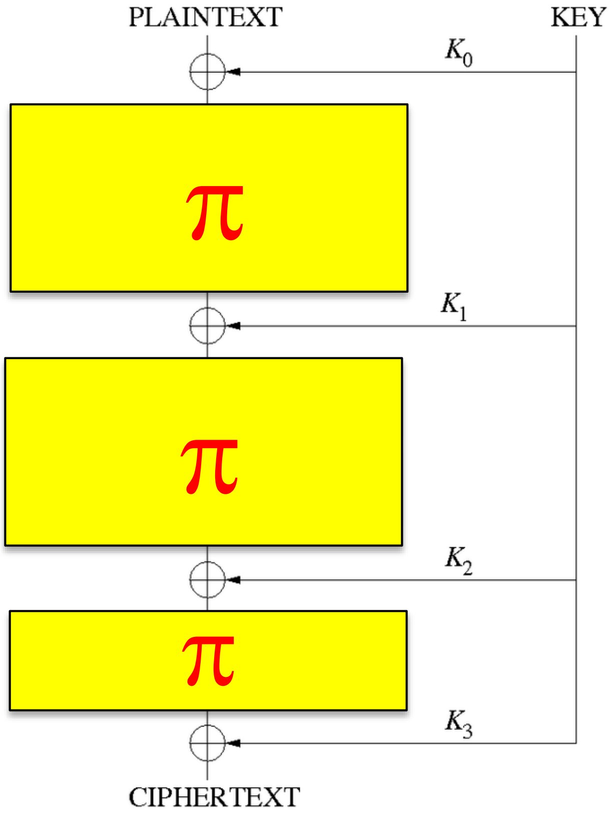
: ~~SPNs~~ KACs (and AES)

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call "SPN"
  - Solution: key alternating ciphers (KAC)



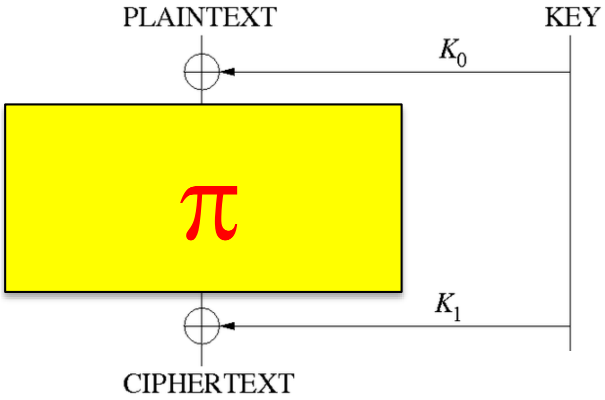
: ~~SPNs~~ KACs (and AES)

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call "SPN"
  - Solution: key alternating ciphers (KAC)
- Prove PRP security in the "big-box" random permutation model (RPM)



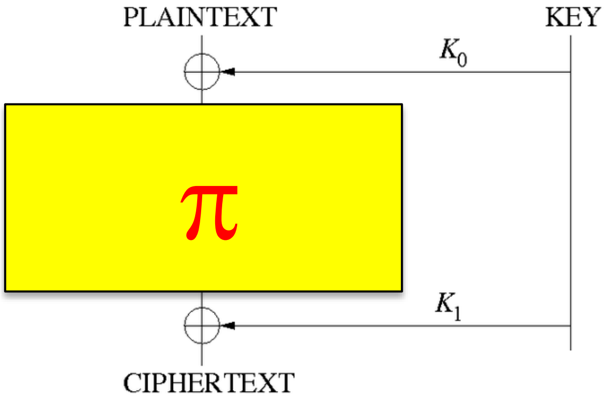
: KACs ~~SPNs~~ (and AES)

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call “SPN”
  - Solution: key alternating ciphers (KAC)
- Prove PRP security in the “big-box” random permutation model (RPM)
  - [EM91]: secure in 1 round!



KACs : ~~SPNs~~ (and AES)

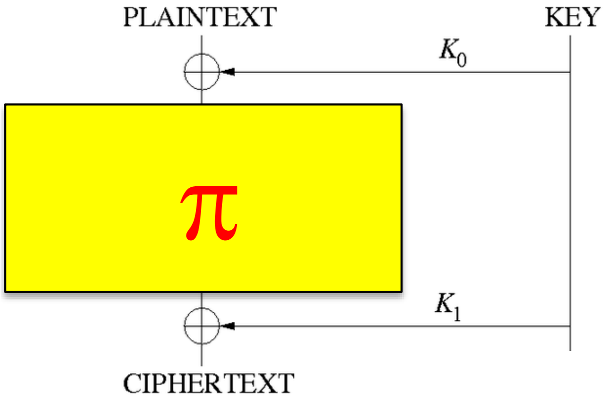
- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call “SPN”
  - Solution: key alternating ciphers (KAC)
- Prove PRP security in the “big-box” random permutation model (RPM)
  - [EM91]: secure in 1 round!



Is this enough for to bring practice to theory?

KACs : ~~SPNs (and AES)~~

- Replace substitution-permutation structure as one big permutation π
  - Problem: no longer can call “SPN”
  - Solution: key alternating ciphers (KAC)
- Prove PRP security in the “big-box” random permutation model (RPM)
  - [EM91]: secure in 1 round!



Is this enough for to bring practice to theory?

Problems with

- Abstracts away SPN structure – heart of design!

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation
- Predicted # of rounds too low (no 1-round SPN is secure!)

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation
- Predicted # of rounds too low (no 1-round SPN is secure!)
  - exact security of KAC increases with number of rounds ☺ [BKL$^+$12,CS14,HT16]

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation
- Predicted # of rounds too low (no 1-round SPN is secure!)
  - exact security of KAC increases with number of rounds ☺ [BKL$^+$12,CS14,HT16]
  - But still with monolithic random permutation(s) ☹

Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation
- Predicted # of rounds too low (no 1-round SPN is secure!)
  - exact security of KAC increases with number of rounds ☺ [BKL$^+$12,CS14,HT16]
  - But still with monolithic random permutation(s) ☹

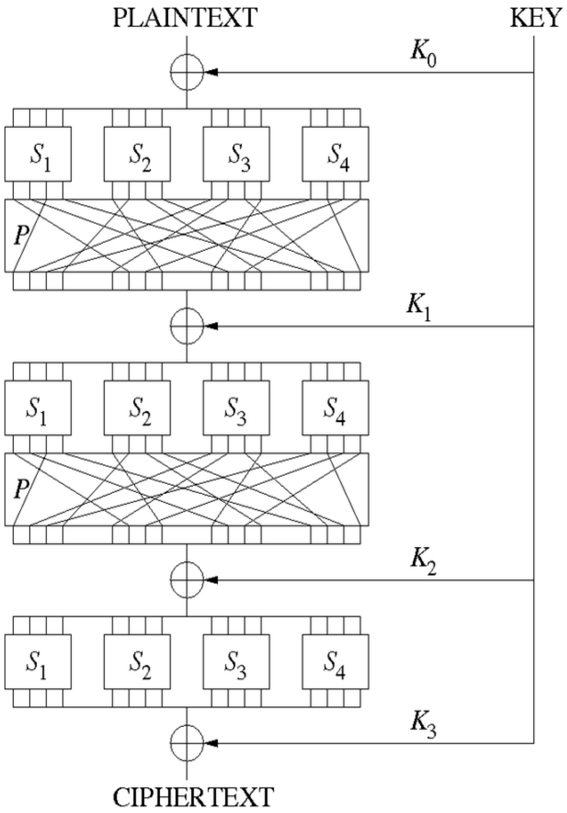
Problems with

- Abstracts away SPN structure – heart of design!
- Cannot implement huge, monolithic random permutation
  - Concrete permutation (e.g. SPN) will never be ideal
  - No guidance which *concrete* choice of π better. Why SPN?
  - Proof guarantees vanish in any concrete implementation
- Predicted # of rounds too low (no 1-round SPN is secure!)
  - exact security of KAC increases with number of rounds ☺ [BKL+12,CS14,HT16]
  - But still with monolithic random permutation(s) ☹
- No (meaningful) quantitative bounds for *exact security* or *number of rounds* with real SPNs

to Practitioners?

GUIDANCE to Practitioners?

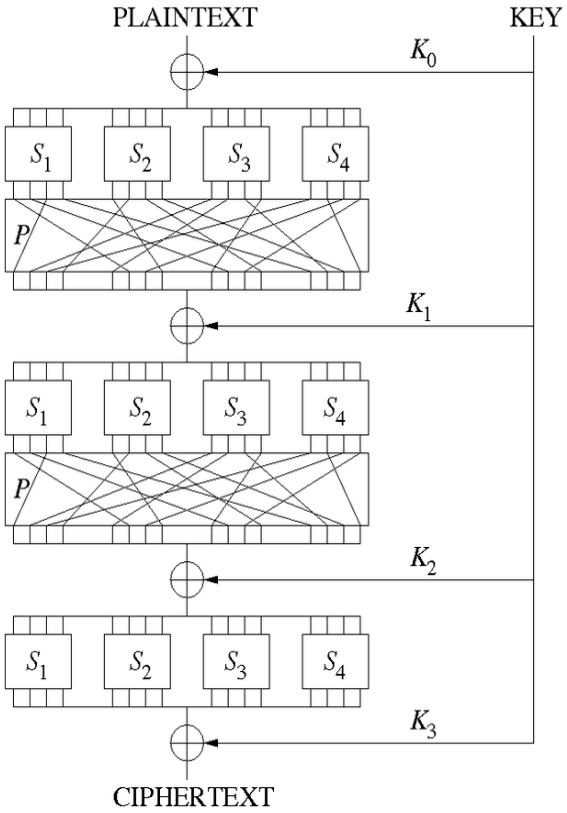
SPN



GUIDANCE to Practitioners?

SPN

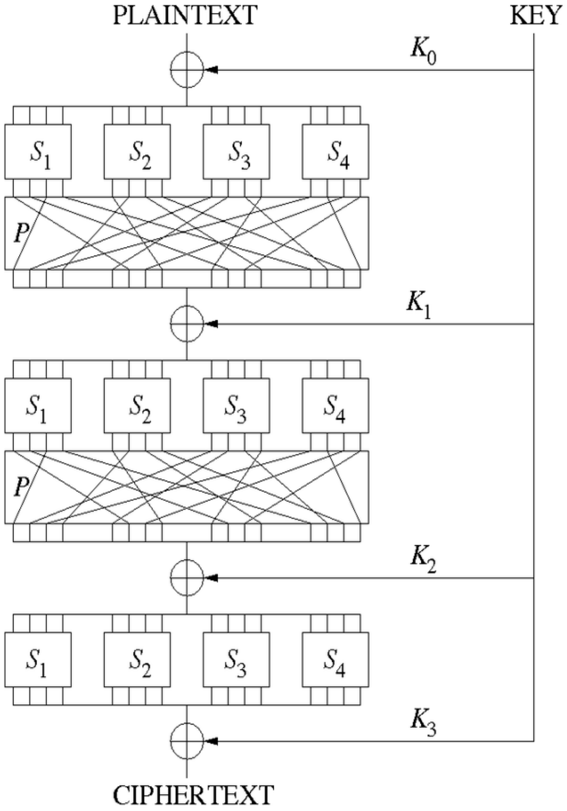
$2^{-8r/3}$ security in r rounds



GUIDANCE to Practitioners?

SPN

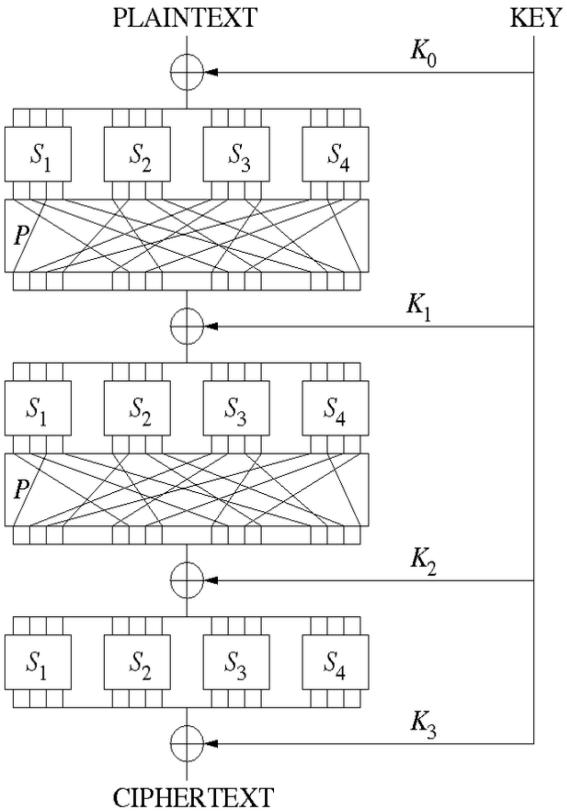
$2^{-8r/3}$ security in r rounds



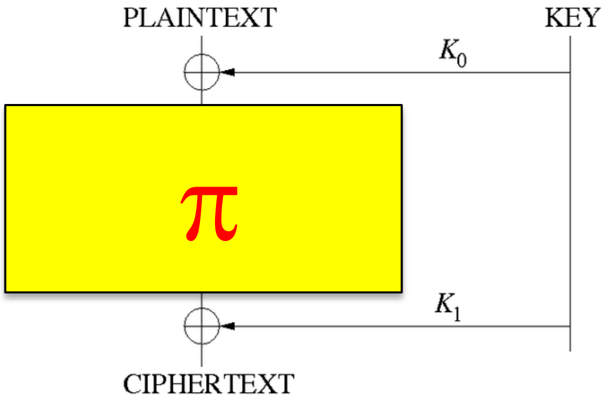
GUIDANCE to Practitioners?

SPN

$2^{-8r/3}$ security in r rounds



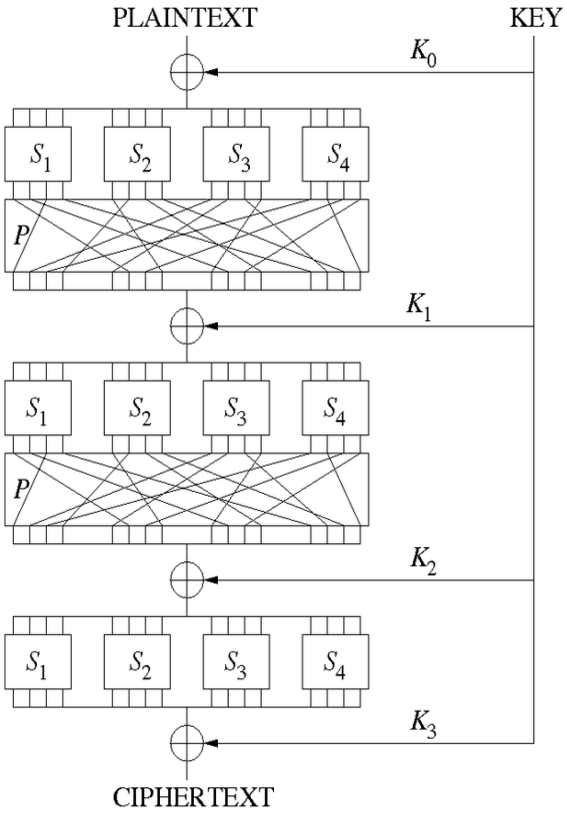
EM



GUIDANCE to Practitioners?

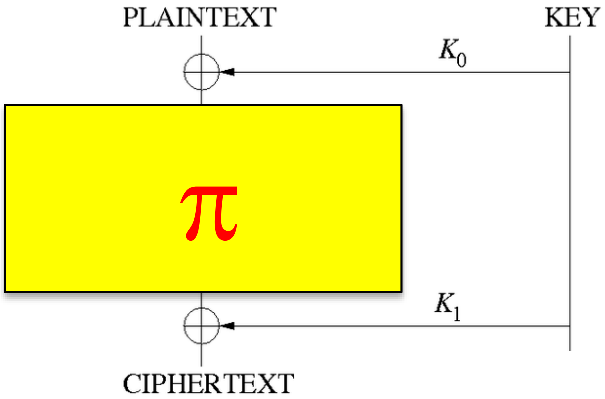
SPN

$2^{-8r/3}$ security in r rounds



EM

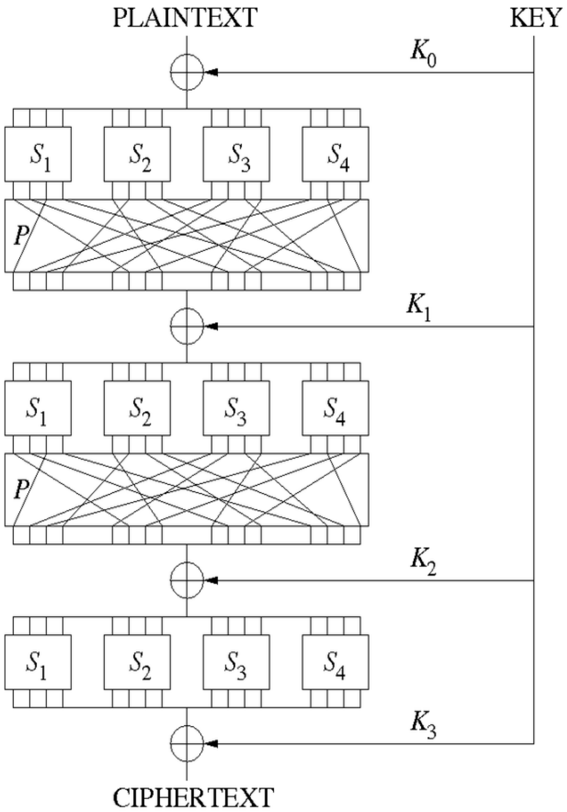
? security in ? rounds with ? π



GUIDANCE to Practitioners?

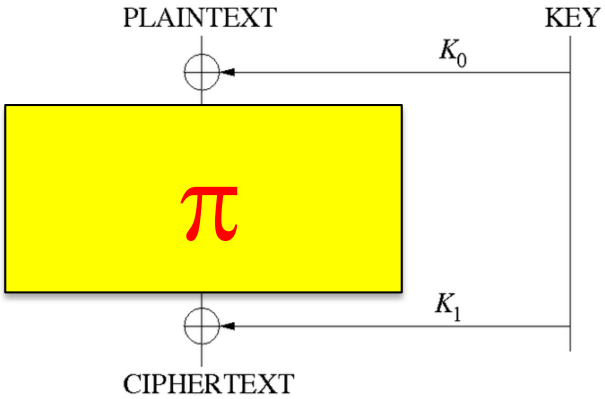
SPN

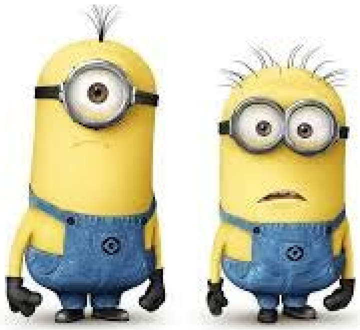
$2^{-8r/3}$ security in r rounds



EM

? security in ? rounds with ? π





Why Better than “AES is secure”?

Why Better than "AES is secure"?

- Small-Box Crypto has large provable component
  - In fact, quite elegant and technically non-trivial

Why Better than “AES is secure”?

It's better to be absolutely ridiculous than absolutely boring.
DespicableMeMinions.org
fb.com/MinionQuote

- Small-Box Crypto has large provable component
  - In fact, quite elegant and technically non-trivial
- Get quantitative bounds *in a systematic way*
  - E.g., dependence on rounds via hardness amplification

Why Better than “AES is secure”?

- Small-Box Crypto has large provable component
  - In fact, quite elegant and technically non-trivial
- Get quantitative bounds *in a systematic way*
  - E.g., dependence on rounds via hardness amplification
- Big-to-Small conjecture is “syntactically natural”:
  - general construction with nice looking security $\varepsilon(n)$ for large n, probably has similar security for small n

The BIGGER PICTURE

- Need theory of hardness from small components

- Need theory of hardness from small components
- Conventional models/assumptions fail

- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to (“OWF” of?) Small-Box Cryptography

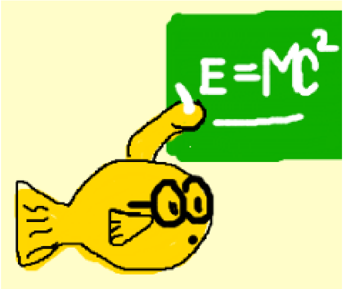
- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to (“OWF” of?) Small-Box Cryptography
- New Philosophy for Design and Analysis:

- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to ("OWF" of?) Small-Box Cryptography
- New Philosophy for Design and Analysis:

Go to BIG-BOX

- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to (“OWF” of?) Small-Box Cryptography
- New Philosophy for Design and Analysis:

Go to BIG-BOX

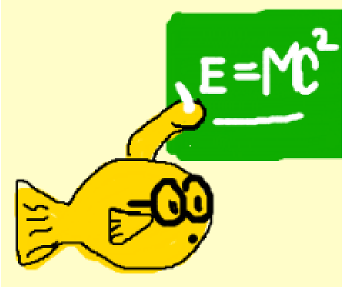


Prove all you can there

The BIGGER PICTURE

- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to ("OWF" of?) Small-Box Cryptography
- New Philosophy for Design and Analysis:

Go to BIG-BOX

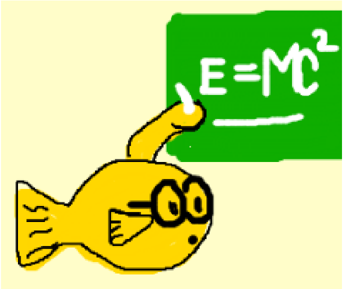


Prove all you can there

Go to small-box

- Need theory of hardness from small components
- Conventional models/assumptions fail
- Big-to-Small Conjecture: new type of assumption friendly to (“OWF” of?) Small-Box Cryptography
- New Philosophy for Design and Analysis:

Go to BIG-BOX



Prove all you can there

Go to small-box

- A lot of work remains (Feistel, Big-to-Small, …)

THANKS!