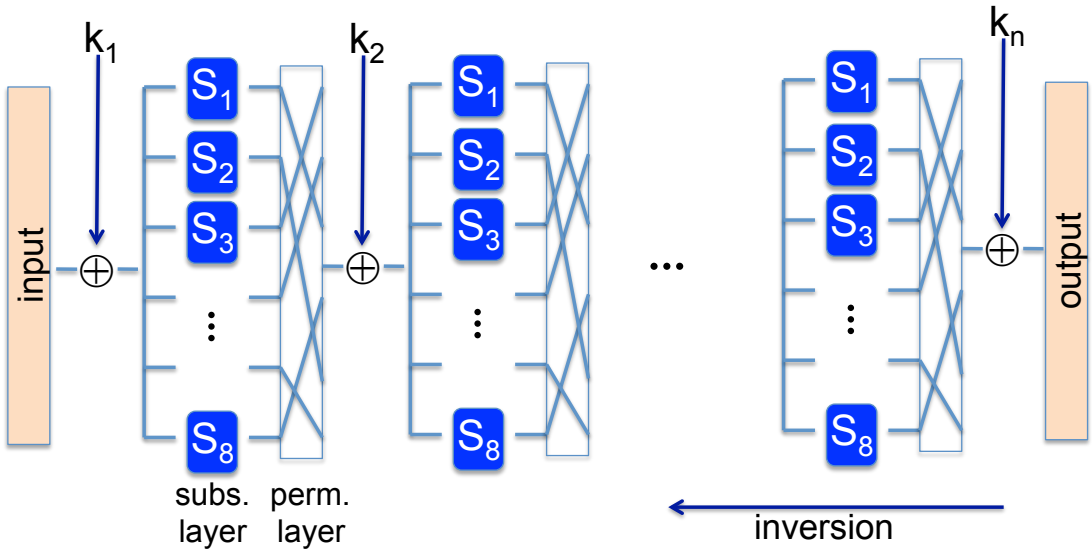
Advanced Encryption Standard (AES)

Symmetric Encryption

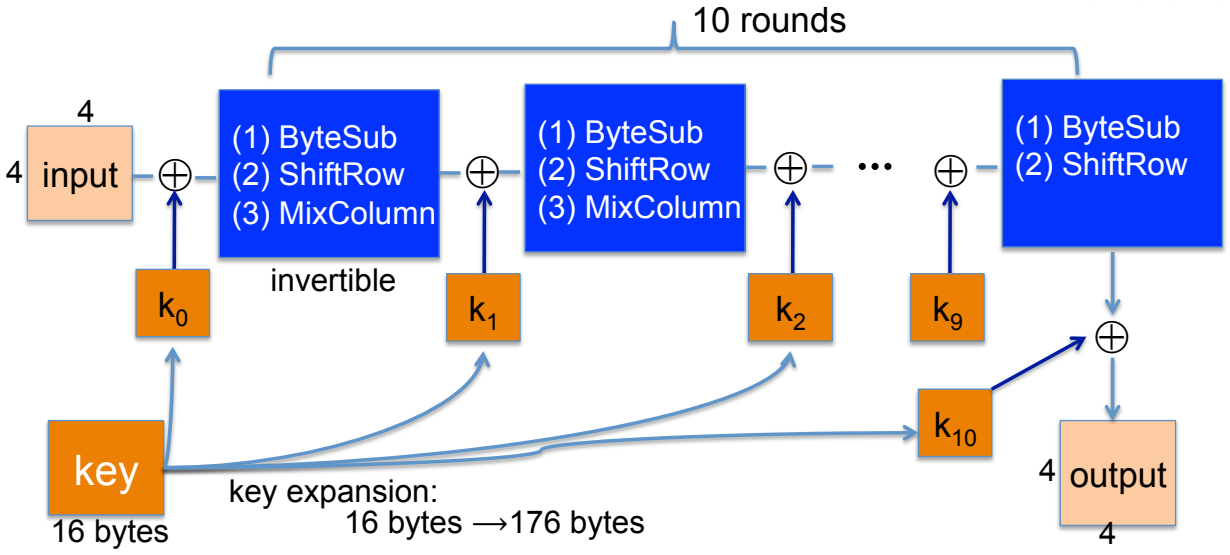
AES history

- 1997: NIST publishes request for proposal
- 1998: fifteen proposals
- 1999: NIST chooses five finalists
- 2000: NIST choses Rijndael as AES
  - Key sizes: 128, 192, 256
    - the longer, the more secure but the slower
  - Block size: 128 bits

AES is a Subs-Perms network (not a Feistel network)



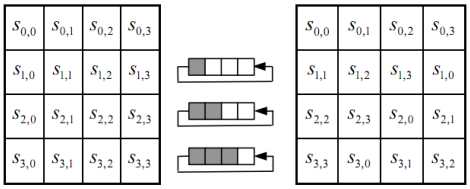
AES-128 schematics



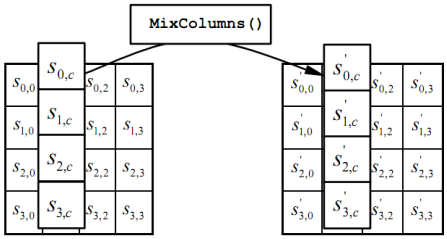
The round function

UNIVERSITÀ DI PISA

- **ByteSub**: a 1-byte S-box (256 byte table)
  - Easily computable
- **ShiftRows:**



- **MixColumns:**
  (linear transformations)



Code size/performance tradeoff

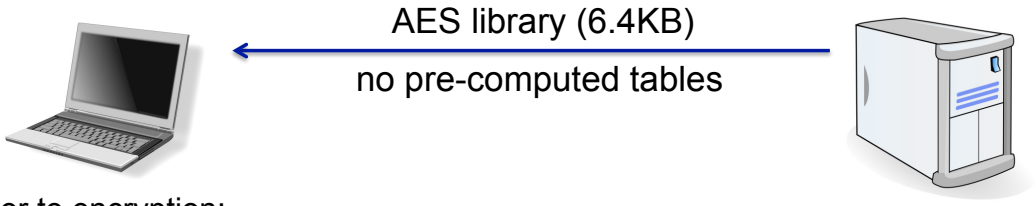
UNIVERSITÀ DI PISA

	Code size	Performance
Pre-compute round functions (24KB or 4 KB)	Largest	Fastest (table lookups and xors)
Pre-compute S-box only (256 bytes)	Smaller	Slower
No pre-computation	Smallest	Slowest

Example: Javascript AES

UNIVERSITÀ DI PISA

AES in the browser:



Prior to encryption:
pre-compute tables

Then encrypt using tables

http://crypto.stanford.edu/sjcl/

AES in hardware

UNIVERSITÀ DI PISA

- AES instructions in Intel Westmere
  - **aesenc**, **aesenclast**: do one round of AES
    - 128-bit registers: **xmm1** = state, **xmm2** = round key
    - **aesenc xmm1, xmm2** puts result in **xmm1**
  - **aeskeygenassist** performs key expansion
  - Implement AES in ten instructions
    - 9x **aesenc** + **aesenclast**
  - Claim 14x speed-up over OpenSSL on the same hw
- Similar instructions for AMD Bulldozer

Best known attacks

UNIVERSITÀ DI PISA

- Best *key recovery* attack
  - Four times better than exhaustive key search
  - 128-bit key → 126-bit key
- *Related key* attack in AES-256
  - Given 2^{99} *pt-ct* pairs from **four related keys** in AES-256, we can recover keys in 2^{99}