lecture10

Advanced Encryption Standard (AES)

128-bit block size

Three key lengths: 128, 192, 256 bits

very efficient & secure

1997 NSIT → New Block cipher call

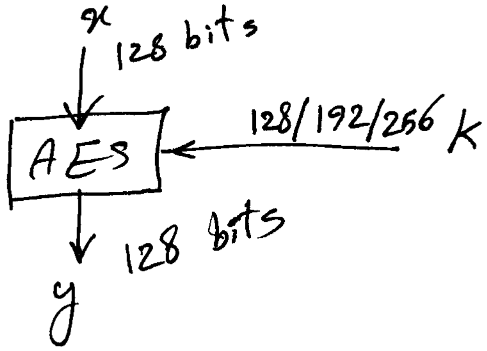
1998 15 Candidates were selected

1999 5 finalist

Mars, RC6, $\underbrace{\text{Rijndael}}_{\text{AES}}$, Serpent, Twofish

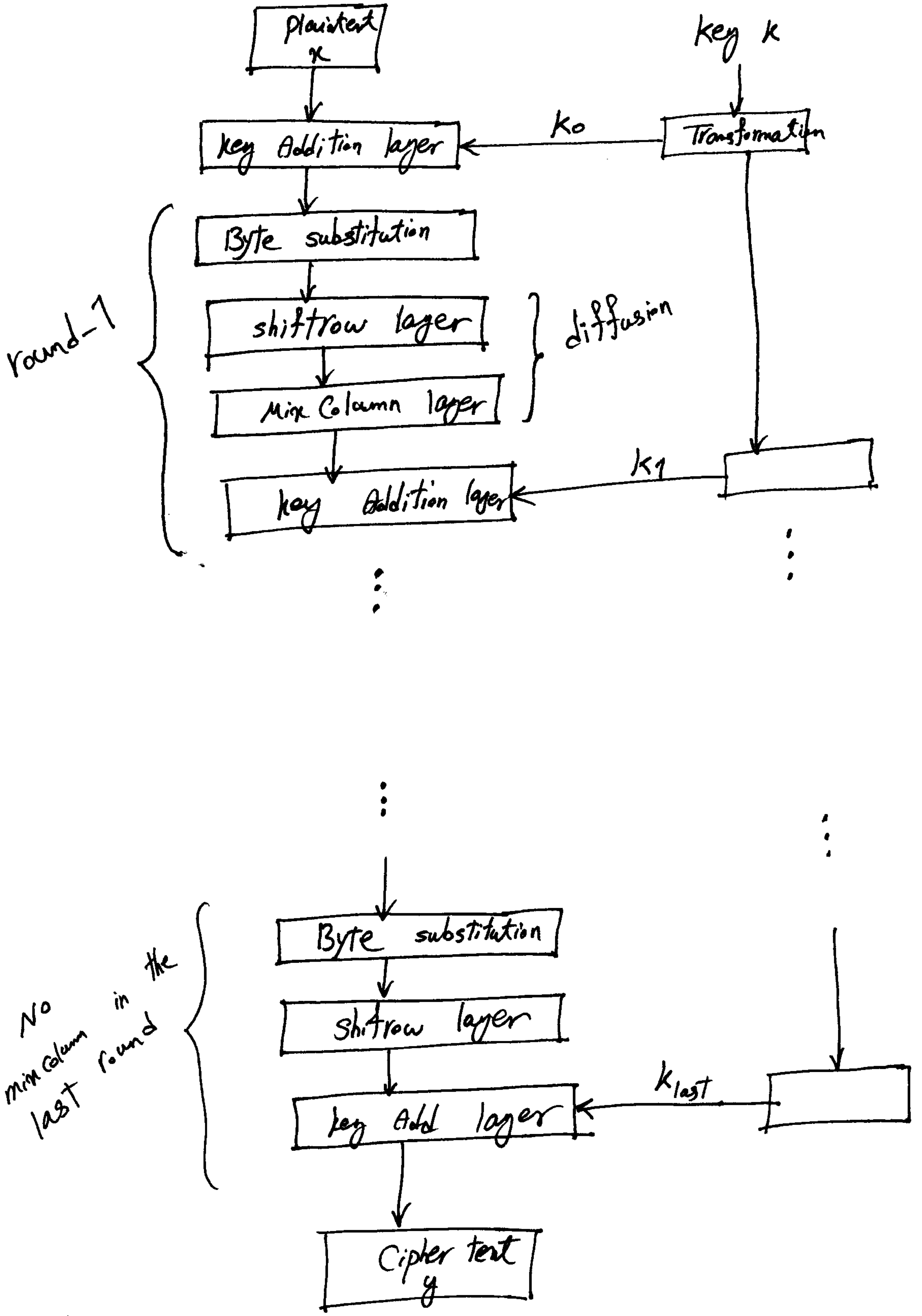
2000 → selected AES

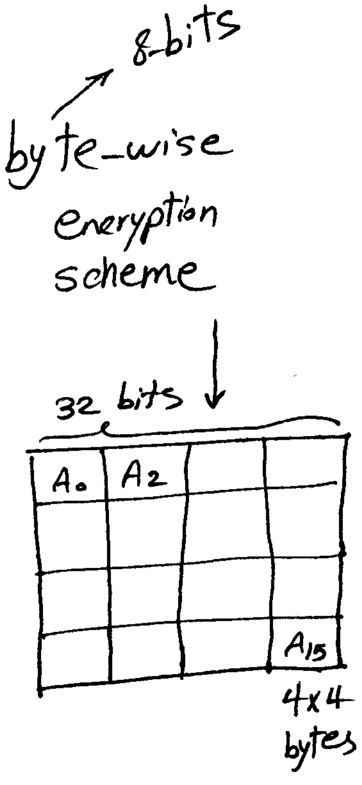
2001 → AES was formally approved



key	rounds
128	10
192	12
256	14

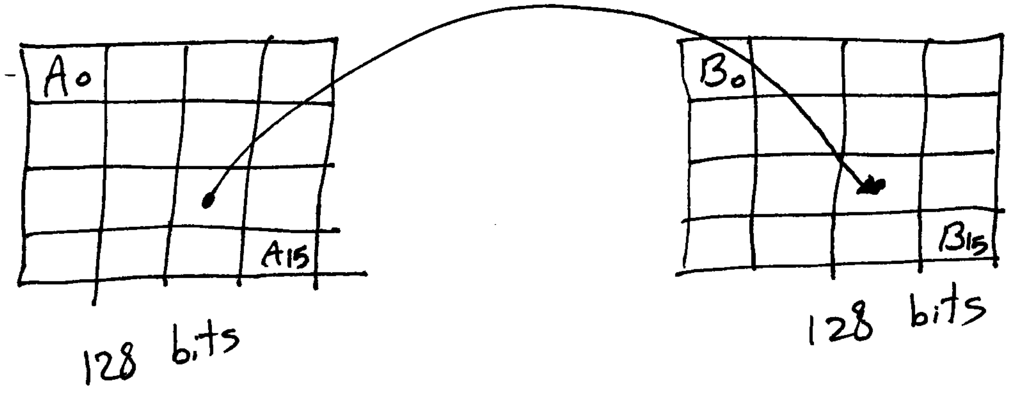
Architecture AES





4×32 bits $= 128$ bits

1. Byte substitution

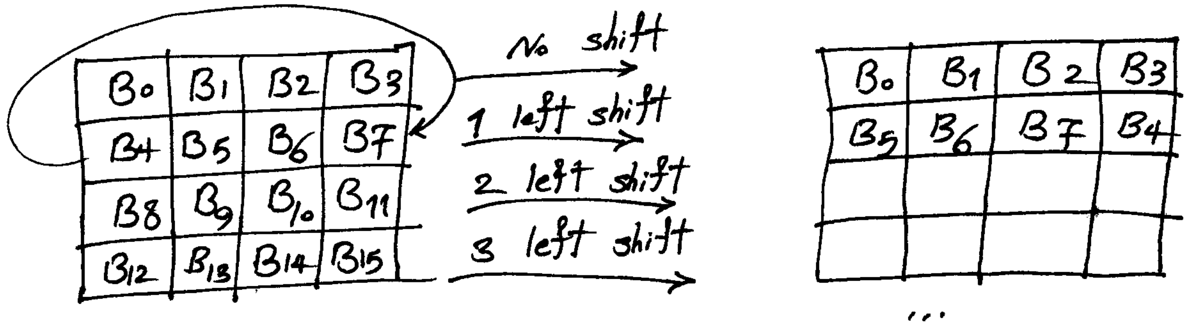


affine transformation

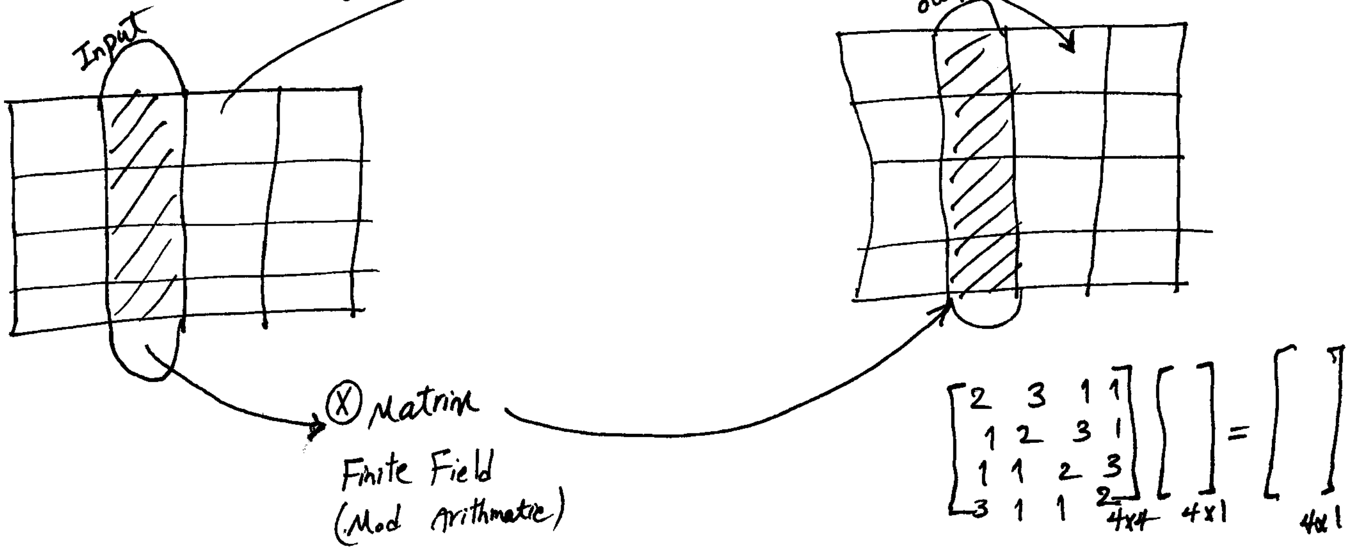
$$f(x) = ax + b \pmod{p}$$

$$\gcd(a, p) = 1$$

2. shiftrow layer

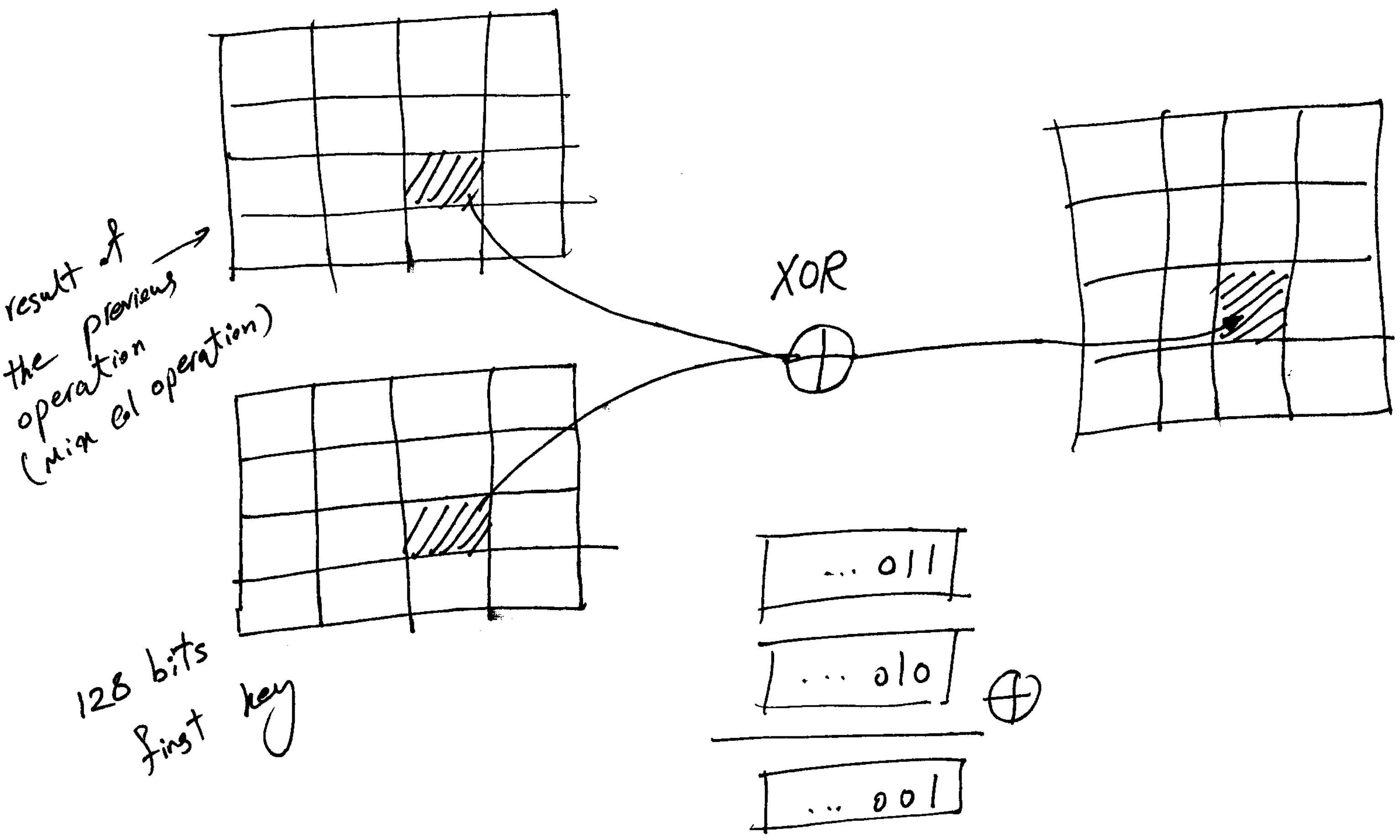


3. Mix column layer



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}_{4\times4} \begin{bmatrix} \\ \\ \\ \end{bmatrix}_{4\times1} = \begin{bmatrix} \\ \\ \\ \end{bmatrix}_{4\times1}$$

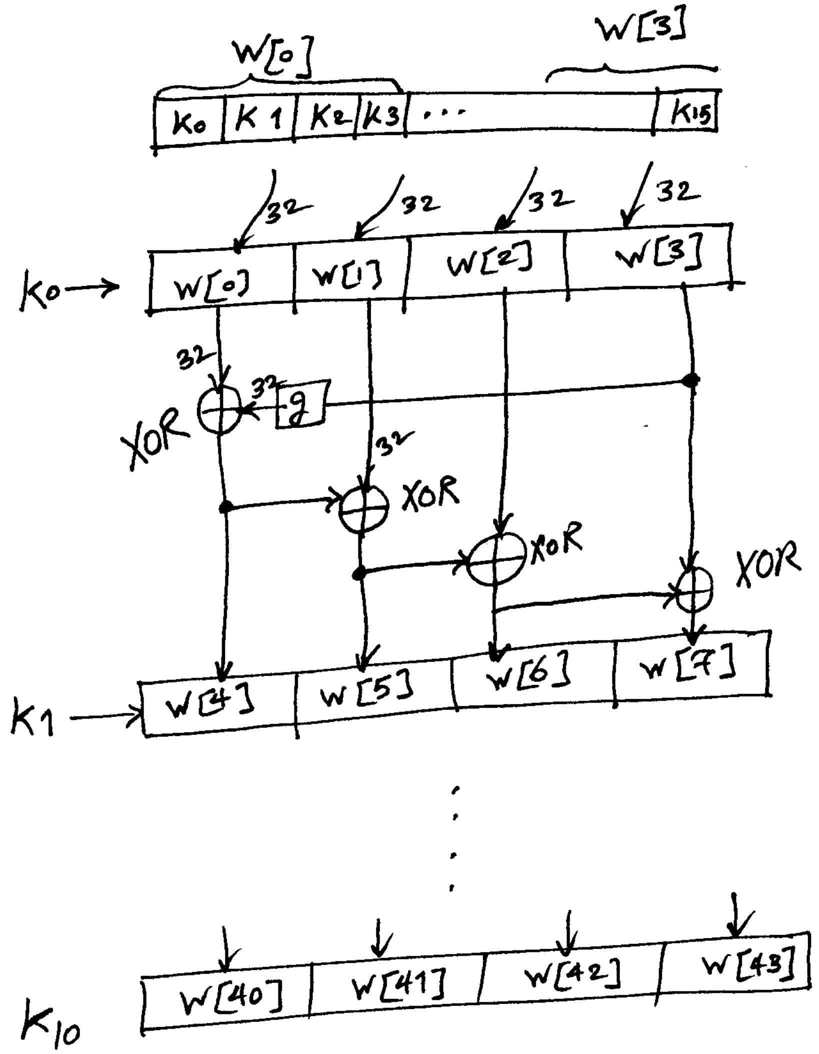
4. key Addition layer



key size	rounds	sub keys $k_0 \sim k_{10}$
128	10	11
192	12	13
256	14	15

key schedule

128-bit key



$16\ \overbrace{\text{Bytes}}^{\text{8-bit}} = 128$ bits

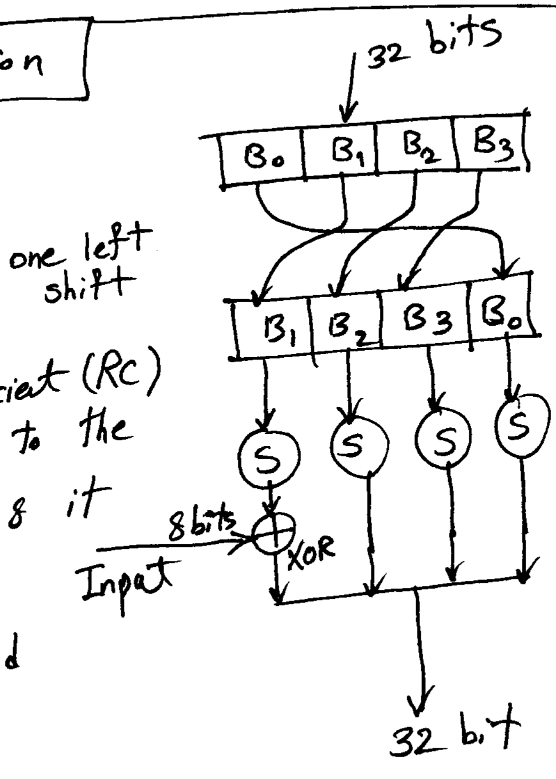
4 bytes → 1 word

10 rounds

11 keys → $K_0 \sim K_{10}$

$\underbrace{\text{44 words in total}}_{\text{11 keys X 4 words}}$

g: function



#the round coefficiet (RC) is only added to the leftmost byte & it varies from round to round

} affine transformation
$f(x)=ax+b \pmod{p}$