OTP and AES: A Historical Transition Between two Systems of Cryptography

Valdemar Thanner
Supervised by Mr. Bernhard Keller
Linguistic supervision by Ms. Margrit Oetiker

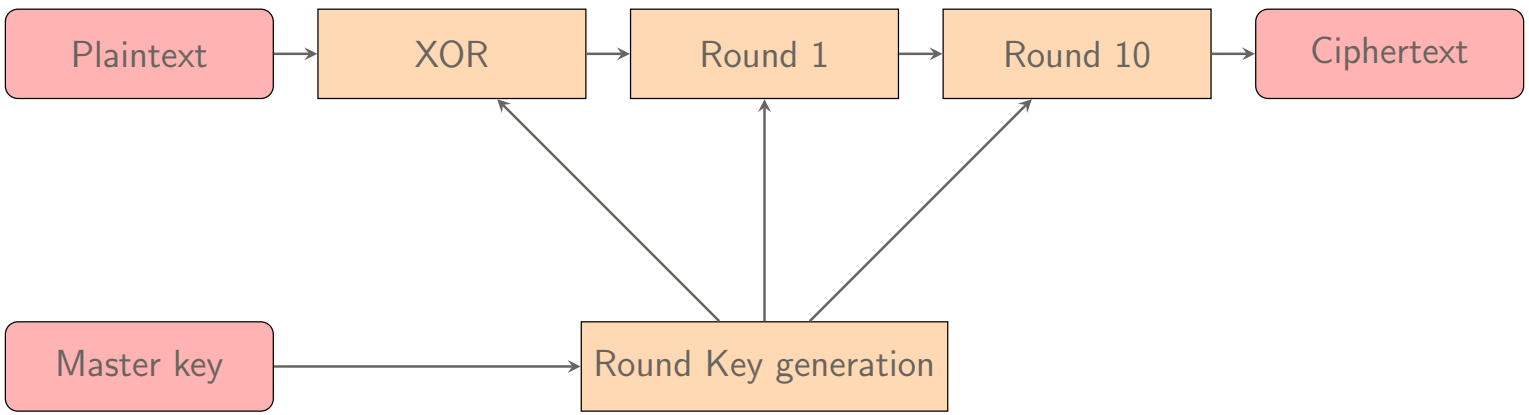
Kantonsschule Zug

06.03.2017

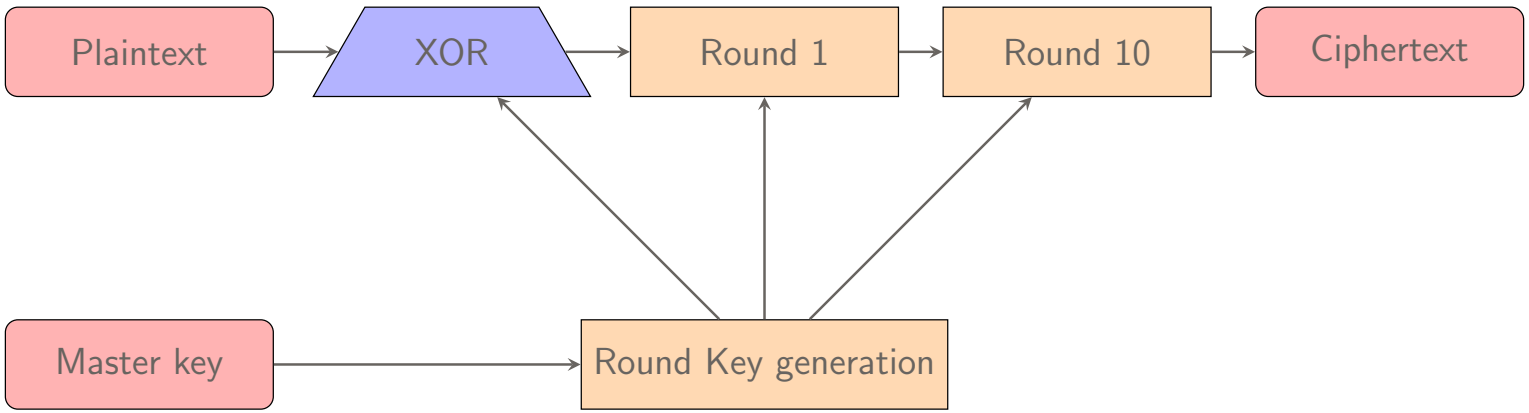
OTP: The One Time Pad

AES: The Advanced Encryption Standard

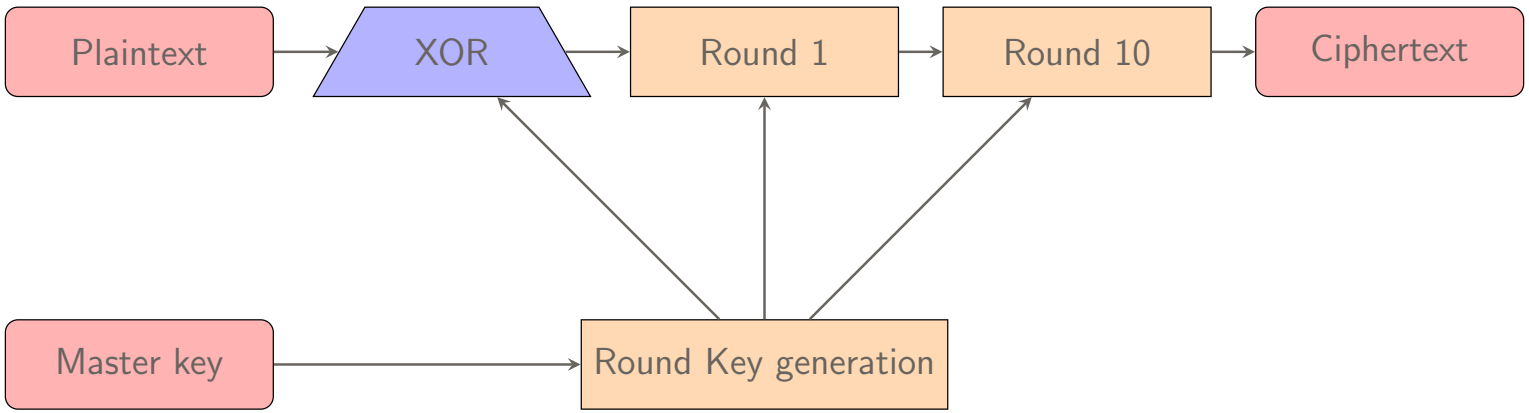
AES: High-Level Structure



AES: Rounds

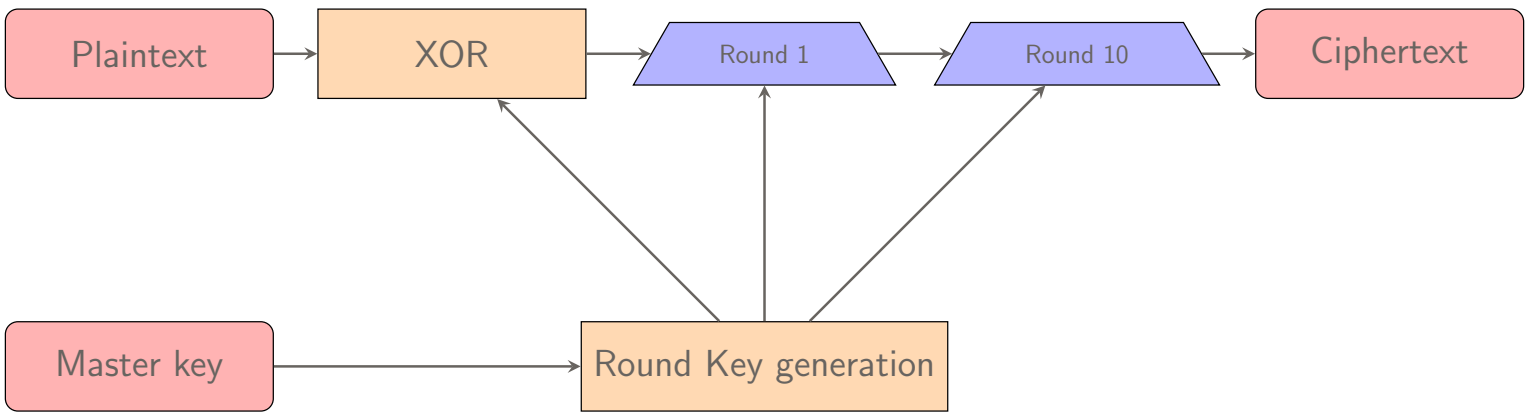

Plaintext
XOR
Round 1
Round 10
Ciphertext
Master key
Round Key generation

AES: Rounds

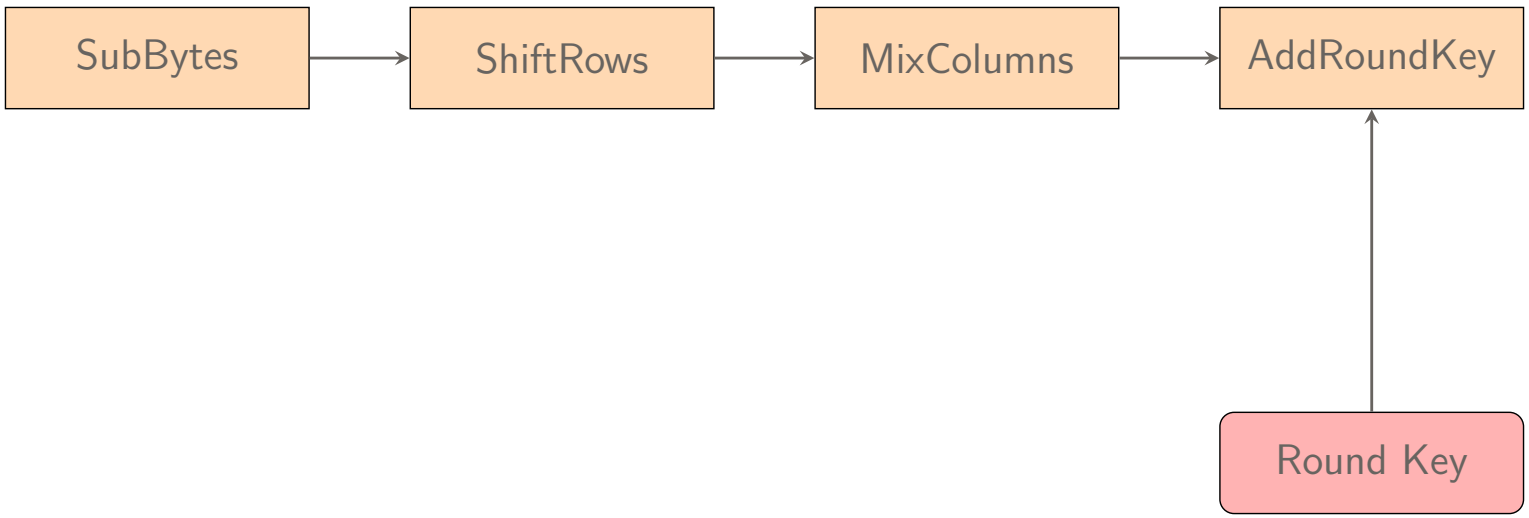


$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ \oplus & \oplus & \oplus & \oplus \\ 0 & 1 & 1 & 0 \\ = & = & = & = \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

AES: Rounds


Plaintext
XOR
Round 1
Round 10
Ciphertext
Master key
Round Key generation

AES: Rounds



AES: SubBytes

AES: ShiftRows

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \xrightarrow{\text{ShiftRows}} \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{pmatrix}$$

AES: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

AES: MixColumns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix}$$

$$\begin{aligned} s_0 &= 02a_0 + 03a_1 + 01a_2 + 01a_3 \\ s_1 &= 01a_0 + 02a_1 + 03a_2 + 01a_3 \\ s_2 &= 01a_0 + 01a_1 + 02a_2 + 03a_3 \\ s_3 &= 03a_0 + 01a_1 + 01a_2 + 02a_3 \end{aligned}$$

AES: AddRoundKey