CODICI SEGRETI

Agostino Dovier

Dip di Matematica e Informatica, Univ. di Udine

Ringrazio l'amico e maestro Andrea Sgarro per il materiale tratto dal suo meraviglioso quanto introvabile testo

Advanced Encryption Standard

Introduzione

- AES fu annunciato dalla NIST come standard nel 2002, dopo diversi di discussioni e una competizione, vinta dall'algoritmo Rijndael
- Gli autori di Rijndael sono i belgi Joan Daemen and Vincent Rijmen.

Advanced Encryption Standard

Introduzione

- Come per il DES, il funzionamento è totalmente pubblico.
- AES è in tre versioni differenziate dalla lunghezza della chiave: AES-128, AES-192 e AES-256.
- La cifrazione avviene comunque sempre con blocchi di 128 bits.
- Usa una “substitution permutation network” invece di una “Feistel network”.
- Può essere esteso con blocchi fino a 256 bits, ma con chiavi di lunghezza illimitata.
- C’è largo uso dell’algebra in $GF(2^8)$.
- Spiegazione originale in: `http://csrc.nist.gov/archive/aes/rijndael/misc/nissc2.pdf`

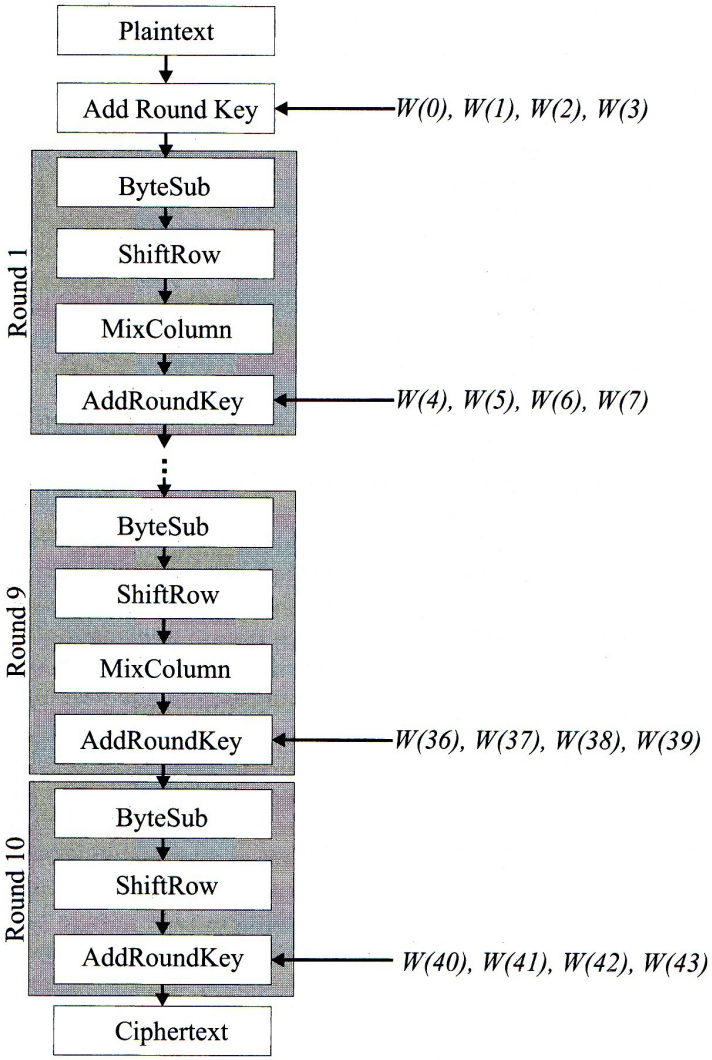
Advanced Encryption Standard

Introduzione

- Come per il DES, il funzionamento è totalmente pubblico.
- AES è in tre versioni differenziate dalla lunghezza della chiave: AES-128, AES-192 e AES-256.
- La cifrazione avviene comunque sempre con blocchi di 128 bits.
- Usa una “substitution permutation network” invece di una “Feistel network”.
- Può essere esteso con blocchi fino a 256 bits, ma con chiavi di lunghezza illimitata.
- C’è largo uso dell’algebra in $GF(2^8)$.
- Spiegazione originale in: `http://csrc.nist.gov/archive/aes/rijndael/misc/nissc2.pdf`

Advanced Encryption Standard

Funzionamento



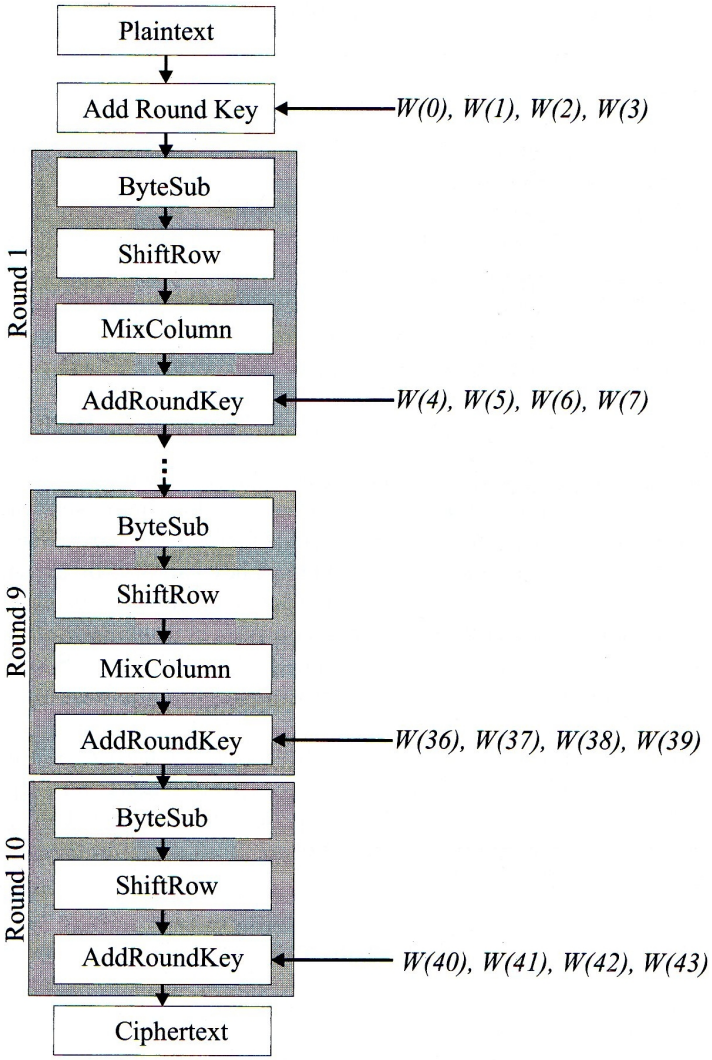
Con la chiave a 128 bits (192, 256), l'algoritmo a sinistra consta di 10 (12, 14) iterazioni.

In ogni iterazione ci sono 4 passi:

1. ByteSub Transformation.
2. ShiftRow Transformation.
3. MixColumn Transformation.
4. AddRoundKey.

Advanced Encryption Standard

Funzionamento



Con la chiave a 128 bits (192, 256), l'algoritmo a sinistra consta di 10 (12, 14) iterazioni.
In ogni iterazione ci sono 4 passi:

1. ByteSub Transformation.
2. ShiftRow Transformation.
3. MixColumn Transformation.
4. AddRoundKey.

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile:$X^8 + X^4 + X^3 + X + 1$

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile:$X^8 + X^4 + X^3 + X + 1$

I 128 input bit sono raggruppati in 16 Bytes:

$$a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, \ldots, a_{2,3} a_{3,3}$$

organizzati in una matrice

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Ogni $a_{i,j}$ è visto come un elemento di $GF(2^8)$ con polinomio irriducibile:$X^8 + X^4 + X^3 + X + 1$

Advanced Encryption Standard

Funzionamento: $GF(2^8)$ con $p(X) = X^8 + X^4 + X^3 + X + 1$

Le somme sono or-esclusivi bit per bit

$$\begin{array}{l} X^7+\quad X^5+X^4+X^3+\quad X+ \\ \quad X^6+X^5+X^4+\quad X^2+X+1= \\ \hline X^7+X^6+\quad X^3+X^2+\quad 1 \end{array} \qquad \begin{array}{r} 10111010\oplus \\ 01110111= \\ \hline 11001101 \end{array}$$

I prodotti sono invece operazioni in $GF(2^8)$ modulo $p(X)$:

$$\begin{array}{l} (X^5+X^4+X^3+\quad X)\times \\ (X^6+\qquad\qquad X)= \\ \hline X^{11}+X^{10}+X^9+\ X^7+X^6+X^5+X^4+X^2= \\ X^6+\ X^5+\ X^4+\quad X^2+X \end{array} \qquad \begin{array}{r} 00111010\times \\ 01000010= \\ \hline 01110110 \end{array}$$

ADVANCED ENCRYPTION STANDARD

FUNZIONAMENTO: $GF(2^8)$ CON $p(X) = X^8 + X^4 + X^3 + X + 1$

Le somme sono or-esclusivi bit per bit

$$\begin{array}{r} X^7+\quad X^5+X^4+X^3+\quad X+ \\ \quad X^6+X^5+X^4+\quad X^2+X+1= \\ \hline X^7+X^6+\quad X^3+X^2+\quad 1 \end{array} \qquad \begin{array}{r} 10111010\oplus \\ 01110111= \\ \hline 11001101 \end{array}$$

I prodotti sono invece operazioni in $GF(2^8)$ modulo $p(X)$:

$$\begin{array}{r} (X^5+X^4+X^3+\quad X) \\ (X^6+\qquad\qquad X) \\ \hline X^{11}+X^{10}+X^9+\ X^7+X^6+X^5+X^4+X^2 \\ \hline X^6+\ X^5+\ X^4+\quad X^2+X \end{array} \begin{array}{l} \times \\ = \\ = \end{array} \begin{array}{r} 00111010\times \\ 01000010= \\ \hline 01110110 \end{array}$$

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.

Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.

Si rappresenta con un byte il numero indicato.

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.

Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.

Si rappresenta con un byte il numero indicato.

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Sia $a_7 \cdots a_0$ un elemento della matrice.
Si guarda la riga $a_7 a_6 a_5 a_4$ e la colonna $a_3 a_2 a_1 a_0$.
Si rappresenta con un byte il numero indicato.

Advanced Encryption Standard

Funzionamento: ByteSub Transformation

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \Longrightarrow \underbrace{\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}}_{B}$$

$$\underbrace{\begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}}_{C} = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{1,0} \\ b_{2,2} & b_{2,3} & b_{2,0} & b_{2,1} \\ b_{3,3} & b_{3,0} & b_{3,1} & b_{3,2} \end{pmatrix}$$

Le righe sono shiftate ciclicamente a sinistra di 0, 1, 2, 3.
Dunque $c_{i,j} = b_{i,(i+j) \mod 4}$

$$\underbrace{\begin{pmatrix} X & X+1 & 1 & 1 \\ 1 & X & X+1 & 1 \\ 1 & 1 & X & X+1 \\ X+1 & 1 & 1 & X \end{pmatrix}}_{D} \times \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

ADVANCED ENCRYPTION STANDARD

FUNZIONAMENTO: ROUNDKEY ADDITION

K, detta RoundKey, è una matrice ottenuta dalla chiave che descriviamo dopo.

$$\underbrace{\overbrace{\begin{pmatrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix}}^{D} \oplus \overbrace{\begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}}^{K}}_{E}$$

E è l'output (128 bit) dell'iterazione.

Advanced Encryption Standard

Funzionamento: Chiave

- La chiave originale è di 128 bits, considerati in una matrice W 4×4 di bytes (o elementi di $GF(2^8)$)
- Siano $W(0), W(1), W(2), W(3)$ le quattro colonne di W
- La matrice è allargata aggiungendo altre 40 colonne $W(4), \ldots, W(43)$ usando la regola:

$$W(i) = \begin{cases} W(i-4) \oplus W(i-1) & \text{Se } i \bmod 4 \neq 0 \\ W(i-4) \oplus T(W(i-1)) & \text{Se } i \bmod 4 = 0 \end{cases}$$

  dove T la vediamo subito.
- La RoundKey per l'iterazione j consiste nella matrice: $(W(4j), W(4j+1), W(4j+2), W(4j+3))$.

Advanced Encryption Standard

Funzionamento: Chiave

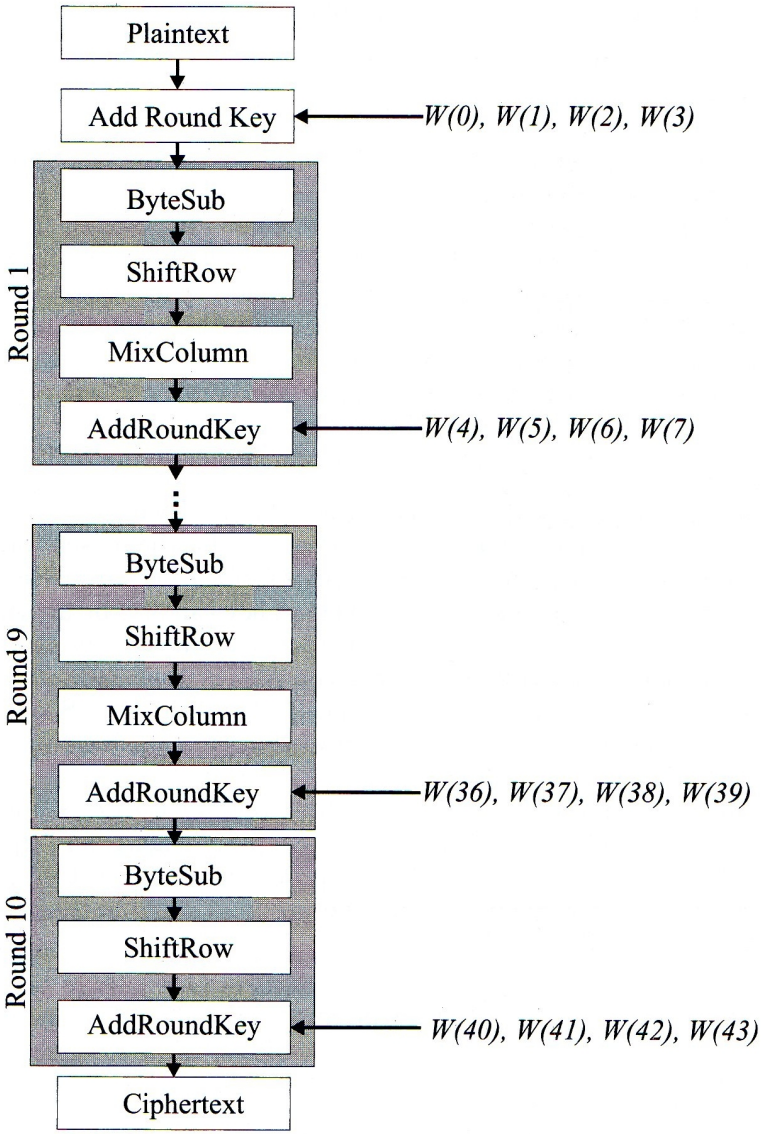
- Definiamo la trasformazione $T(W(i))$ (i multiplo di 4).
- $W(i)$ viene shiftato ciclicamente e poi sostituto usando la S-Box:

$$W(i) = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \overset{\text{shift}}{\Longrightarrow} \begin{pmatrix} b \\ c \\ d \\ a \end{pmatrix} \overset{\text{S-Box}}{\Longrightarrow} \begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix}$$

- Si calcola $r(i) = X^{\left(\frac{i-4}{4}\right)}$ in $GF(2^8)$
- Si definisce $T(W(i)) = \begin{pmatrix} e \oplus r(i) \\ f \\ g \\ h \end{pmatrix}$

Advanced Encryption Standard

Funzionamento: Riassunto



Advanced Encryption Standard

Decifrazione

- Le varie operazioni sono invertibili.
- C'è l'inversa della S-Box
- C'è l'inversa della ShiftRow (basta shiftare a dx)
- C'è l'inversa della MixColumn (la matrice è invertibile)
- Per la RoundKey si usa la stessa.

Advanced Encryption Standard

Decifrazione

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.
Il fatto che non siano uguali è un punto di forza.

ADVANCED ENCRYPTION STANDARD

DECIFRAZIONE

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.

Il fatto che non siano uguali è un punto di forza.

ADVANCED ENCRYPTION STANDARD

DECIFRAZIONE

Cifrazione
ARK(0–3)
BS,SR, MC, ARK (4–7)
⋮
BS,SR, MC, ARK (36–39)
BS,SR, ARK (40–43)

Decifrazione
ARK (40–43), ISR, IBS
ARK (36–39), IMC, ISR, IBS
⋮
ARK (4–7), IMC, ISR, IBS
ARK (0–3)

Si può lavorare sulla decifrazione in modo da renderla un pò più simile (ma non uguale) alla cifrazione.
Il fatto che non siano uguali è un punto di forza.

Advanced Encryption Standard

Funzionamento: S-Box

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Advanced Encryption Standard

Funzionamento: S-Box

- La matrice S-Box non è casuale.
- Consideriamo il byte $\vec{b} = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$
- Sia $\vec{e} = e_7 e_6 e_5 e_4 e_3 e_2 e_1 e_0$ il suo inverso in $GF(2^8)$ (assumiamo che l'inverso di $\vec{0}$ sia lui stesso).
- Passare all'inverso spezza sia attacchi lineari, che differenziali, che di interpolazione.
- $\vec{z}$ si ottiene moltiplicando una matrice (simmetrica) per $\vec{e}$ e sommando al risultato il vettore $(1, 1, 0, 0, 0, 1, 1, 0)$.
- $z_7 z_6 z_5 z_4 z_3 z_2 z_1 z_0$ è la entry nella S-box.

Advanced Encryption Standard

Considerazioni finali

- S-Box che usa l'inverso spezza sia attacchi lineari, che differenziali, che di interpolazione.
- ShiftRow serve a resistere a due attacchi denominati *differenziali troncati* e *square*.
- MixColumn serve a spargere rapidamente la chiave tra i vari bits
- Il numero di iterazioni (10, 12, 14) serve in quanto ci sono attacchi migliori della forza bruta per 6 iterazioni. 10 è un valore di tranquillità.

Anche qui ci sta bene un laboratorio avanzato. Sugli attacchi effettuati e/o su un tentativo di attacco di forza bruta magari su AES con meno livelli (3/4).

Advanced Encryption Standard

Considerazioni finali

- S-Box che usa l'inverso spezza sia attacchi lineari, che differenziali, che di interpolazione.
- ShiftRow serve a resistere a due attacchi denominati *differenziali troncati* e *square*.
- MixColumn serve a spargere rapidamente la chiave tra i vari bits
- Il numero di iterazioni (10, 12, 14) serve in quanto ci sono attacchi migliori della forza bruta per 6 iterazioni. 10 è un valore di tranquillità.

Anche qui ci sta bene un laboratorio avanzato. Sugli attacchi effettuati e/o su un tentativo di attacco di forza bruta magari su AES con meno livelli (3/4).