3DES (Triple DES) - 1

Per superare la **debolezza** del **DES** a 56 bit una semplice idea è quella di usare N volte il DES portando la **chiave** a **Nx56 bit**.

Nel 1999 fu introdotto il cifrario **3DES** (**Triple DES**) che consiste nel applicare **tre** volte l'algoritmo **DES** alternando la funzione di **cifratura** ***Cifra(chiave,blocco)*** e quella di **decifratura** ***Decifra(chiave,blocco)***, usando tre diverse chiavi a 56 bit.

La cifratura mediante **triplo DES** si articola nei seguenti passi:

C = E(K3,D(K2,E(K1,M)))

dove **M** è il messaggio in **chiaro**, E(K1,M) indica la cifratura di M mediante la chiave K1, D(K2,E(K1,M)) indica la decifratura del messaggio precedentemente criptato, utilizzando questa volta la chiave k2, ed infine, E(K3,D(K2,E(K1,M))) indica la cifratura del messaggio appena decriptato, però mediante la chiave K3. Per capire meglio tale sequenza di operazioni, è conveniente illustrare la seguente schematizzazione:

3DES (Triple DES) - 2

La **decifratura** consiste nelle stesse operazioni della **cifratura**, ma utilizza le **chiavi** in **ordine inverso**:

M = D(K1, E(K2, D(K3,C)))

dove **C** è il messaggio **cifrato**.

Tale operazione viene rappresentata di seguito:

In questo modo la chiave viene ad essere di **3x56 = 168 bit** con molta maggiore sicurezza; il vantaggio è che non è necessario progettare ed implementare nuovi algoritmi o circuiti, si riutilizzano quelli del DES, tali e quali.

In base alla **scelta** delle **chiavi** il **3DES** offre tre alternative:

- Le **tre** chiavi K1, K2 e K3 sono **diverse** ed indipendenti (sicurezza = 168 bit).
- **Due** chiavi **uguali** (K1=K3) ed una diversa (K2) (sicurezza = 112 bit).
- Le **tre** chiavi **tutte uguali** (K1=K2=K3) (sicurezza=56 bit come il DES).

Oggi il **3DES** viene utilizzato con alcune varianti nelle transazioni commerciali elettroniche (**VISA**, **Mastercard**..).

IDEA (International Data Encryption Algorithm)

Nel 1991 fu proposto il cifrario **IDEA** in sostituzione del **DES**, proprio quando si temeva che lo stesso non avrebbe resistito per molto agli attacchi dei crittoanalisti.

Il metodo progettato in **Svizzera** al politecnico di **Zurigo** ad opera di due famosi ricercatori **Xuejia Lai** e **James Massey** si basa su concetti **simili al DES** con chiave a **128 bit** dove i blocchi del messaggio a **64 bit** vengono elaborati in **8 iterazioni** usando operazioni di **XOR**, **somma** e **moltiplicazione modulo 2^{16}**.

I 64 bit del messaggio vengono divisi in 4 gruppi di 16 bit mescolati con 6 chiavi di 16 bit estratte dalla chiave di 128 bit.

L'algoritmo è uno dei più resistenti e ad oggi non risulta che sia stato violato: i progettisti di **IDEA** lo hanno realizzato in modo che fosse praticamente immune ad attacchi condotti con la **crittoanalisi differenziale** (la crittoanalisi **differenziale** di una funzione crittografica è lo studio di come le differenze nei dati forniti in ingresso alla funzione **possono incidere sulle differenze risultanti** in uscita dalla stessa: l'attaccante deve essere in grado di ottenere i messaggi cifrati relativi a testi in chiaro di sua scelta). Per attacchi a **forza bruta** si calcola che la violazione di una chiave a 128 bit impieghi nel migliore dei casi 2×10^{15} anni per la riuscita. Attualmente è uno dei cifrari a chiave segreta **più utilizzati** per quanto riguarda i software commerciali di crittografia vista la sua **velocità di codifica** e **decodifica** e la sua **elevata sicurezza**.

AES (Advanced Encryption Standard) - 1

Nel **1997** il **NIST** (**National Institute of Standards and Technology**) ha cominciato a cercare ufficialmente un successore per l'oramai anziano standard di crittografia **DES** organizzando un concorso.

Si presentarono 15 candidati: dopo lunghi test e rigorose analisi nel 2000 vinse l'algoritmo di **Rijndael** proposto da due crittografi belgi, **Joan Daemen** e **Vincent Rijmen**. L'**AES - Rijndael** fu certificato nel 2001 come nuovo standard di cifratura. Il nome **Rijndael** è una **sintesi** dei nomi dei suoi inventori.

Si basa su tre caratteristiche fondamentali:

- Resistenza contro gli attacchi.
- Velocità e compattezza del codice su un ampia gamma di piattaforme.
- Semplicità progettuale.

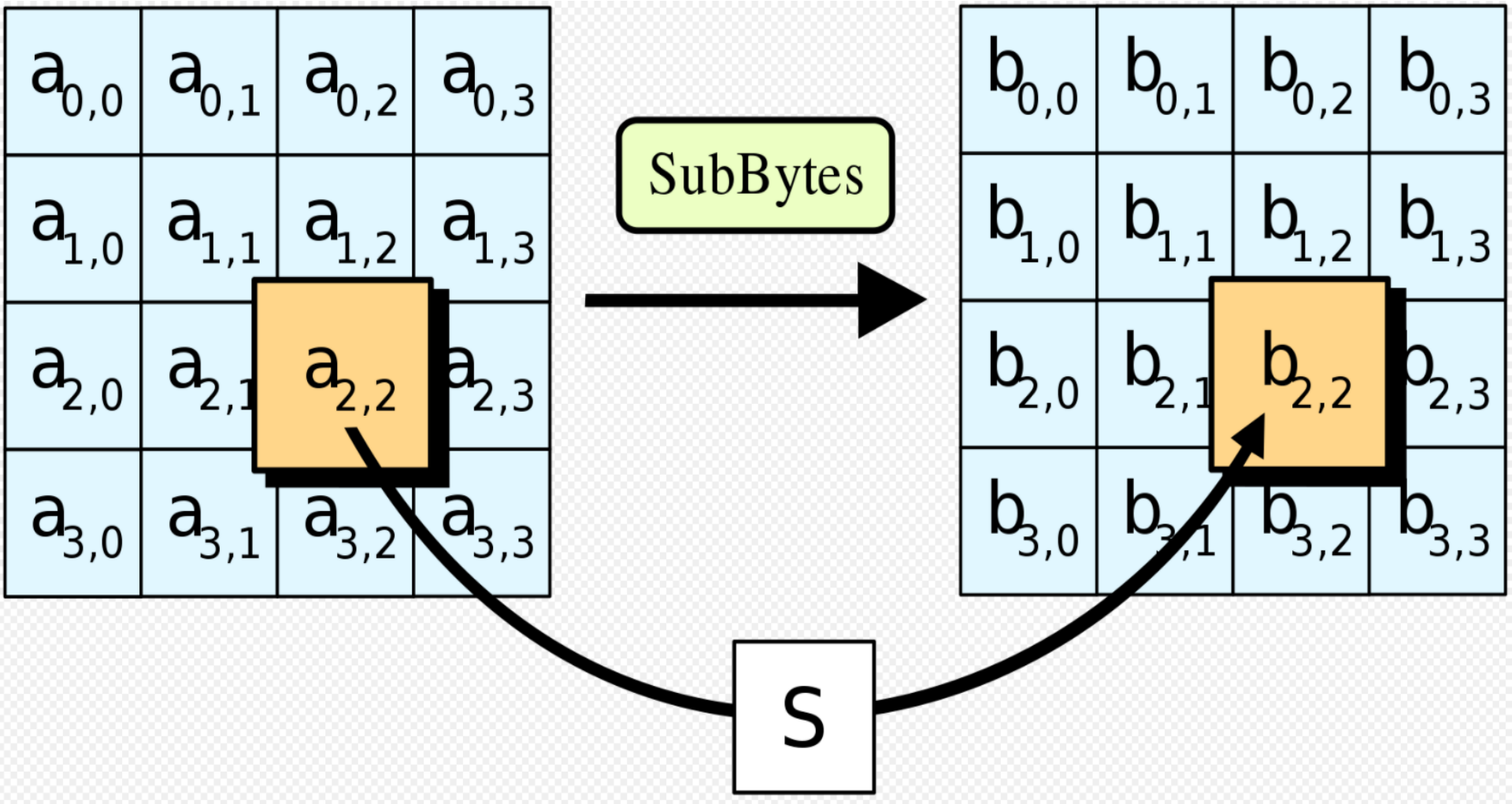
AES è un cifrario a blocchi con **lunghezza del blocco di 128 bit**, ma può avere chiavi indipendenti con lunghezza di 128, 192 e 256 bit, ed effettua una combinazione di **permutazioni** e **sostituzioni**. Come il **DES** prevede la ripetizione di numerosi cicli identici: per l'**AES** a 128, 192 e 256 bit sono previste rispettivamente 10, 12 e 14 **ripetizioni** del ciclo base (**round**).

Ogni blocco di 128 bit è diviso in 16 bytes da 8 bit, che dobbiamo immaginare disposti su una **matrice 4x4 byte**.

AES (Advanced Encryption Standard) - 2

Le **quattro operazioni** che costituiscono **ogni round** sono le seguenti:

1. Substitute Bytes: ogni **byte** viene **trasformato** mediante una permutazione non lineare di byte che vengono mappati tramite una tabella **S-box** a 8 bit definita in **AES** stesso.



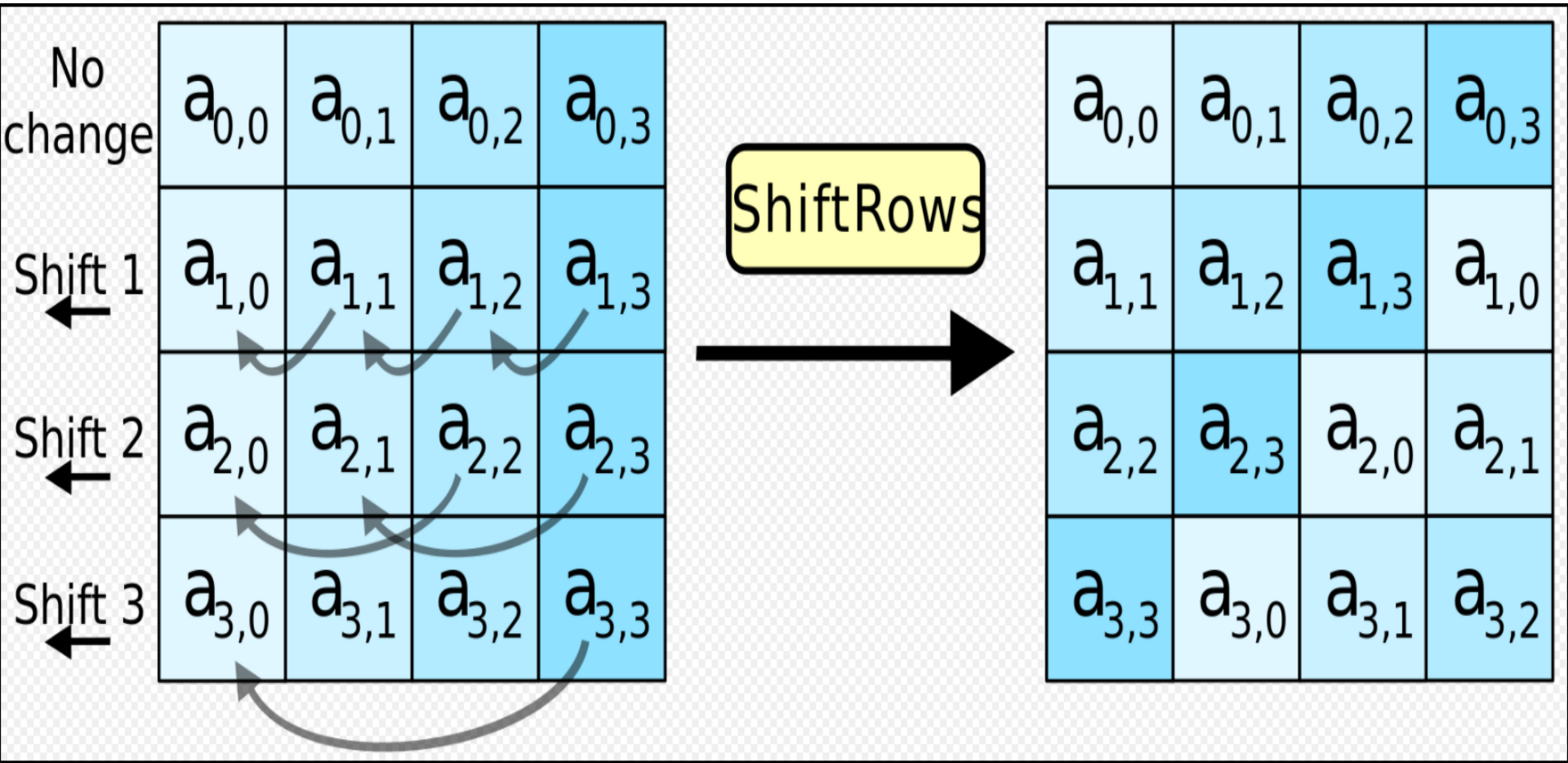
AES (Advanced Encryption Standard) - 3

Tabella **S-box** ad 8 bit usata nell'operazione di **Substitute Bytes**

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

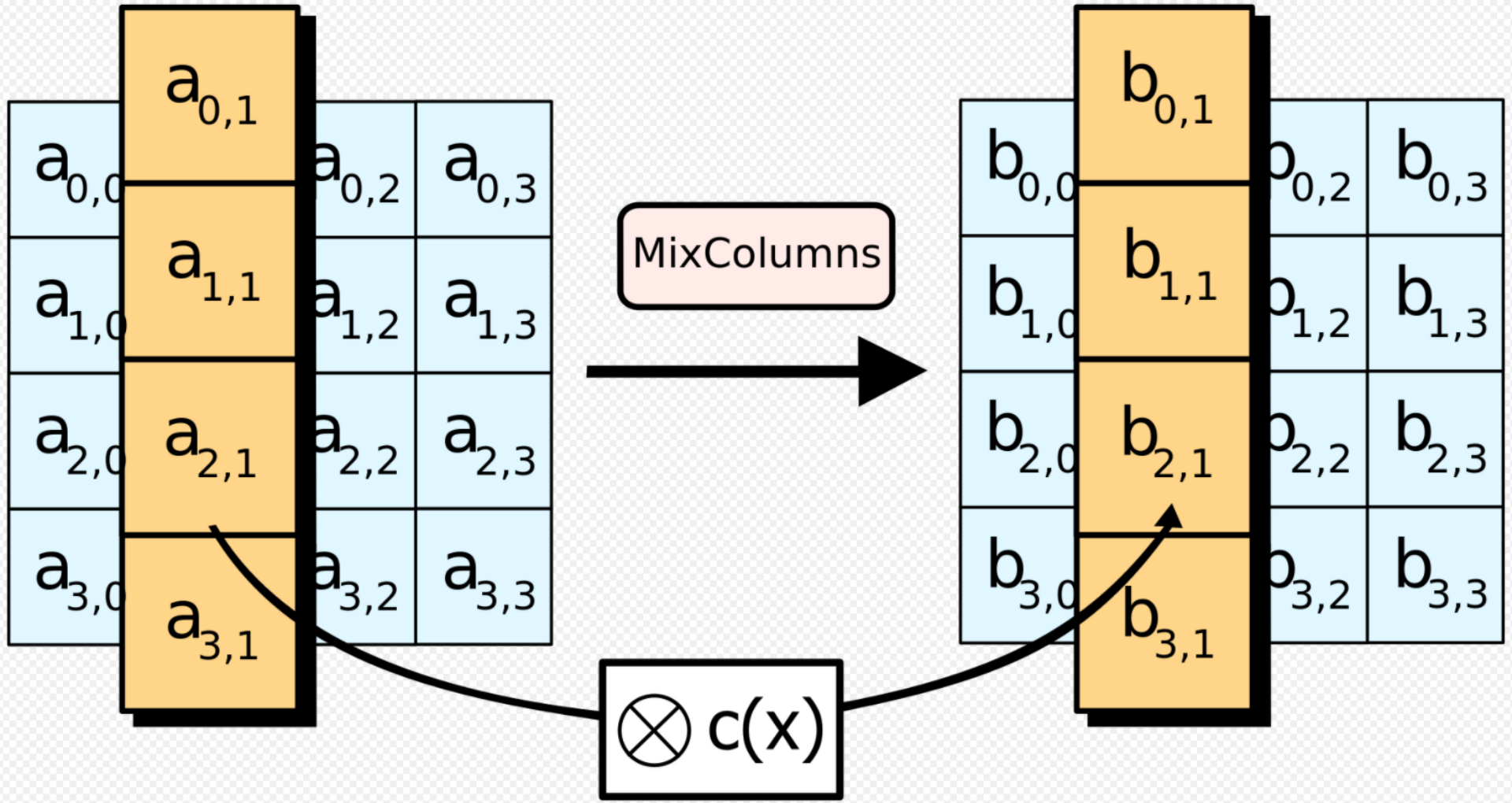
AES (Advanced Encryption Standard) - 4

2. Shift Rows : il passaggio **Shift Rows** provvede a scostare le righe della matrice di un parametro dipendente dal numero di riga. Nell'**AES** la prima riga resta invariata, la seconda viene spostata di un posto verso sinistra, la terza di due posti e la quarta di tre. In questo modo l'ultima colonna dei dati in ingresso andrà a formare la **diagonale** della matrice in uscita.



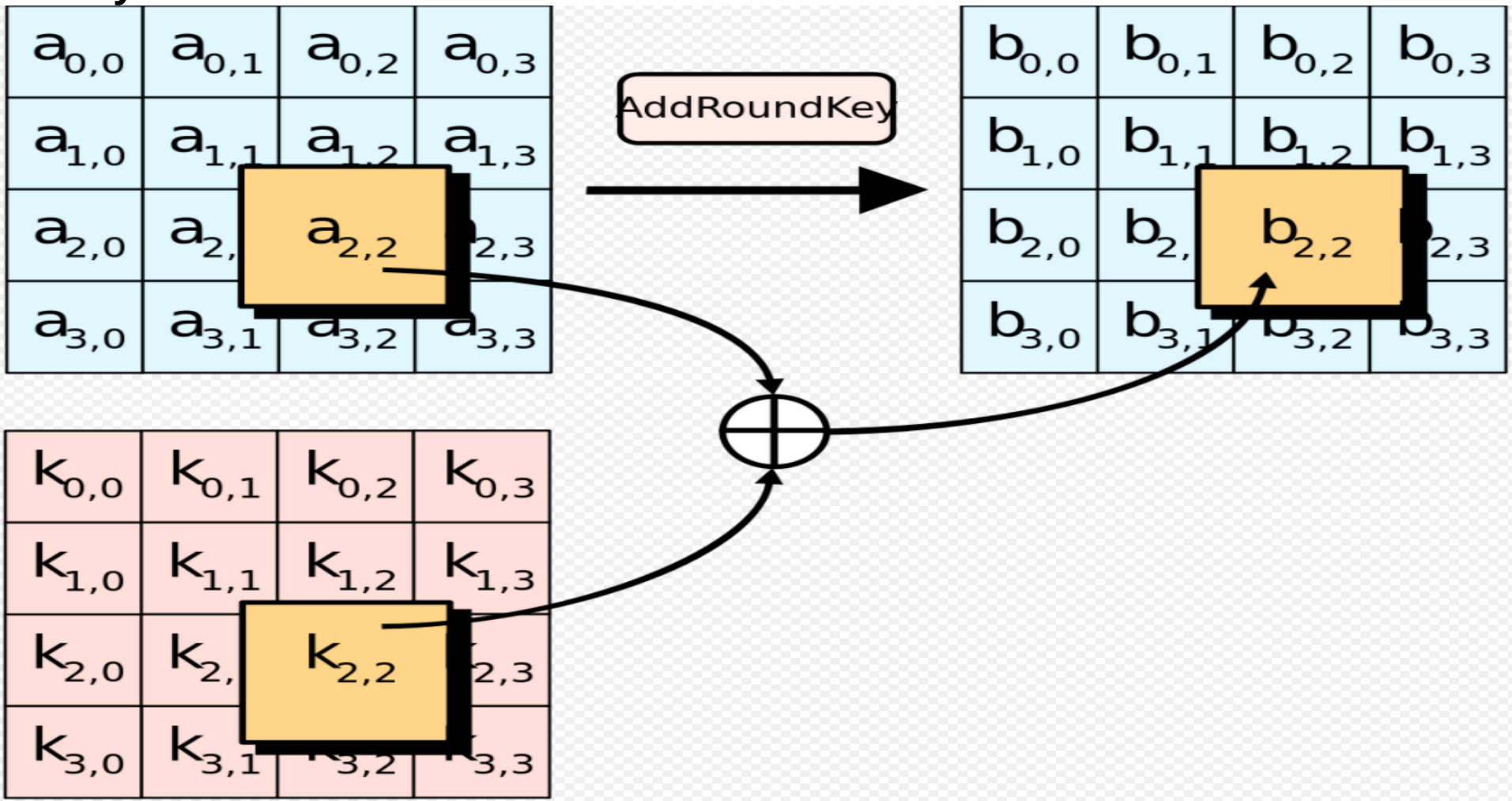
AES (Advanced Encryption Standard) - 5

3. Mix Columns: ogni colonna viene trasformata mediante un'operazione che può essere vista come una **moltiplicazione matriciale** con una particolare matrice generata da un **polinomio prefissato** c(x).



AES (Advanced Encryption Standard) - 6

4. Add Round Key: il passaggio **Add Round Key** combina con uno **XOR** la **chiave di sessione** con la **matrice** ottenuta dai passaggi precedenti . Una chiave di sessione viene **ricavata** dalla **chiave primaria** ad ogni round (con dei passaggi più o meno semplici, ad esempio uno shift di posizione dei bit) grazie al **Key Schedule.**



AES (Advanced Encryption Standard) - 7

La **National Security Agency** (**NSA**) segnalava che tutti i finalisti del processo di standardizzazione erano dotati di una sicurezza sufficiente per **diventare** l'**AES**, ma che fu scelto il **Rijndael** per via della sua flessibilità nel trattare chiavi di lunghezza diversa, per la sua semplice implementazione in **hardware** e in **software** e per le sue basse richieste di memoria che ne consentono un'**implementazione anche** in dispositivi con **scarse risorse come le smart card**. Anche considerando che la potenza dei computer aumenta nel tempo, servirà ancora molto tempo prima che una chiave da 128 bit sia attaccabile con il metodo **forza bruta**.

Nel 2011 è stato pubblicato Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger (2011) ***Biclique Cryptanalysis of the Full AES*** che richiede qualcosa come 2^{126} operazioni per forzare una chiave AES a 128 bit, 2^{190} per AES 192 bit e 2^{254} per AES a 256 bit.

Il **livello** di **sicurezza** di **AES** sembra quindi **molto elevato**; per i documenti del governo USA, **AES 128 bit** è considerato sufficiente per i documenti classificati "**Secret**", mentre per i "**Top Secret**" occorre **AES 192 bit** o meglio ancora **AES 256 bit**.