

Standard di crittografia pubblica: DES, AES

Lezione 6 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Studi in Informatica applicata, AA 2006-7

Indice

1. Standard di crittografia pubblica: DES, AES
2. DES, cenni storici e requisiti
3. l'algoritmo DES
4. DES doppio e triplo, validità di DES
5. AES, cenni storici e requisiti
6. l'algoritmo AES: Rijndael
7. validità di Rijndael
8. riferimenti

DES, cenni storici e requisiti

Data Encryption Standard (DES): il primo standard per la crittografia pubblica
1972: il **National Bureau of Standards (NBS)** degli Stati Uniti pubblica un primo bando per un algoritmo di crittografia per uso pubblico

motivazione : proliferazione di sistemi di crittografia commerciali → incompatibilità

1974: un secondo bando NBS ha miglior fortuna: risponde IBM, suggerendo una variante del suo algoritmo **Lucifer**, già pubblicato in precedenza

1976: il **Data Encryption Algorithm (DEA)** proposto da IBM, superata l'analisi della **National Security Agency (NSA)**, è adottato come standard federale **DES**

requisiti posti nel bando NBS per l'algoritmo:

ad alto livello di sicurezza

specificato e facilmente comprensibile

pubblicabile (sicurezza indipendente dalla segretezza dell'algoritmo)

disponibile a tutti gli utenti

adattabile all'uso per molteplici applicazioni diverse

economico da implementare

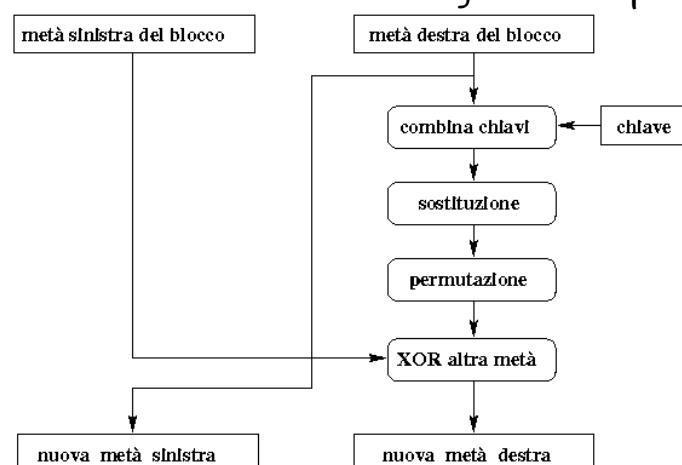
efficiente nell'uso

convalidabile

esportabile

l'algoritmo DES

DES opera una cifratura **simmetrica a blocchi**, di 64 bit ciascuno, con **chiave da 56 bit** su ciascun blocco, la cifratura DES combina **sostituzione e trasposizione** (permutazione del blocco), e inoltre, dopo una permutazione iniziale, opera **16 iterazioni** di tale combinazione (seguite da una permutazione finale):



schema di massima del ciclo DES di sostituzione e permutazione

DES doppio e triplo, validità di DES

la più discussa vulnerabilità di DES è dovuta alla limitata lunghezza della chiave:

l'esplorazione di 2^{56} possibilità, per violare la chiave in un attacco a testo in chiaro e testo cifrato, è alla portata della tecnologia attuale

1997: prima violazione ufficiale di una chiave DES, con un algoritmo eseguito in parallelo da 3500 macchine in 4 mesi;

1998: macchina ad hoc (costo ~100 kEUR) viola una chiave DES in 4 giorni

problema: l'algoritmo DES non si generalizza a una maggiore lunghezza della chiave

soluzione n. 1, DES doppio : $DES2(k_1, k_2, M) = DES(k_2, DES(k_1, M))$

non ha la forza del raddoppio di lunghezza della chiave:

Merkle & Hellman (1981): un attacco al **testo in chiaro conosciuto** genera 2^{56} cifrature DES del testo in chiaro e 2^{56} decifrazioni DES del testo cifrato: si trova la coppia di chiavi con algoritmi efficienti di ricerca di coincidenze

soluzione n. 2, DES triplo : $DES3(k_1, k_2, M) = DES(k_1, DES^{-1}(k_2, DES(k_1, M)))$

più sicuro di DES2, ma **non** ha la forza del raddoppio di lunghezza della chiave:

debolezza simile a quella di DES2, ma per attacco al **testo in chiaro scelto**,
v. Merkle & Hellman (1981)

AES, cenni storici e requisiti

Advanced Encryption Standard (AES):

l'intrinseca vulnerabilità di DES, anche se di rilevanza pratica solo nel medio-lungo periodo, giustifica la ricerca di uno standard più sicuro per la crittografia pubblica

1997: bando del National Institute of Standards and Technology (NIST)

USA per un nuovo algoritmo pubblico di crittografia

1998: selezione di 15 algoritmi fra quelli sottoposti

1999: riduzione della selezione a 5 finalisti, per analisi pubblica e privata

2001: adozione ufficiale dell'algoritmo **Rijndael**, proposto dai crittografi olandesi Vincent Rijmen e Joan Daemen, quale standard AES

tutti gli algoritmi finalisti soddisfacevano tutti i requisiti posti nel bando: scelta finale determinata da **efficienza e semplicità** di implementazione di Rijndael
requisiti posti nel bando NIST per l'algoritmo:

non segreto

divulgato pubblicamente

disponibile per l'uso mondiale senza diritti di sfruttamento

per cifratura simmetrica a blocchi, con blocchi da 128 bit

usabile con chiavi da 128, 192 e 256 bit

l'algoritmo AES: Rijndael

come DES, Rijndael combina sostituzione e trasposizione, con operazioni elementari di scorrimento, XOR, etc., in più iterazioni, però:

il numero delle iterazioni dipende dalla lunghezza della chiave: 9, 11, 13, rispettivamente per lunghezza della chiave pari a 128, 192, 256 bit

ad ogni iterazione si impiega una chiave specifica, o **sottochiave**, derivata da (una porzione della) chiave

ogni iterazione opera in sequenza quattro trasformazioni sul blocco:

sostituzione dei byte: confusione diretta

scorrimento delle righe: il blocco è diviso in 4 righe di equal lunghezza, a ciascuna delle quali si applica uno scorrimento circolare di diversa entità

mescolamento delle colonne: scorrimento e XOR → diffusione

aggiunta della sottochiave (XOR)

la base matematica di Rijndael è nella teoria dei campi di Galois

validità di Rijndael

l'algoritmo Rijndael soddisfa i tre criteri di validità per sistemi di crittografia commerciale, sebbene sia da considerare ancora relativamente giovane

a fronte della sua relativa novità, va tenuto in conto che:

ha superato le crittoanalisi, pubbliche e di esperti, nel periodo di valutazione è stato prodotto da crittografi indipendenti dal committente (governo USA) a differenza di DES, è basato su un metodo matematico generale, che può essere applicato anche:

per lunghezze della chiave superiori a quelle specificate
con un numero maggiore di iterazioni

dunque è ben protetto contro le minacce che conseguono dalla "legge di Moore"

riferimenti

Merkle & Hellman (1981) :

On the Security of Multiple Encryption,

Comm. of the ACM **24**(7), 465-467, 1981.

<http://portal.acm.org/citation.cfm?id=358718&dl=ACM&coll=portal>

Daemen & Rijmen (1999) :

The Rijndael Block Cipher: AES Proposal,

Document version 2, NIST, 03/09/1999.

<http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>

Daemen & Rijmen (2000) :

The Block Cipher Rijndael,

in: Smart Card. Research and Applications, Springer, LNCS **1820**, 277-284, 2000.

<http://www.springerlink.com/content/978-3-540-67923-3>

AES Lounge :

IAIK Krypto Group, TU Graz

<http://www.iaik.tu-graz.ac.at/research/krypto/AES>