Università degli Studi di "Roma Tre"
Elementi di Crittografia
a.a. 2004/2005

CRITTOGRAFIA NELL'AMBITO DELLE SMART CARD

Sicurezza, tecniche di attacco e qualche scenario specifico

Autori: Parisi Francesca
Naclerio Fabio
Paternesi Noemi
Di Maria Valerio

0 Descrizione delle Smart Card

0.1 Possibili Impieghi
0.2 Applicazioni commerciali
0.3 Applicazioni multiple

1 Tipi di Smart Card

1.1 A contatto o senza contatto
1.2 A memoria o microprocessore

2 Struttura Logica

3 Il Sistema Operativo

4 Sicurezza nelle Smart Card

4.1 Integrità dei dati
4.2 Autenticazione
4.3 Irriproducibilità
4.4 Riservatezza

5 Sicurezza Fisica

6 Sicurezza Logica

6.1 Gli Oggetti della Sicurezza
6.2 Smart Card come Motori Crittografici
6.3 Librerie Crittografiche
6.4 Rapporto tra PKI e Smart Card

7 Lettori di Smart Card

7.1 Dumb mouse
7.2 Simple PC Reader
7.3 Smarty
7.4 Software universale PIC/EEPROM del CCC

8 Algoritmo DSA (cenni)

9 Algoritmo MD5 (cenni)

10 Carta d'Identità Elettronica (CIE)

10.1 L'architettura
10.2 Metacomandi CIE
10.3 Struttura delle informazioni sulla banda ottica
10.4 Sicurezza del supporto fisico
10.5 Affidabilità dei dati
10.6 Algoritmi utilizzati
10.A Bibliografia

11 Il telefono e la crittografia

11.1 La sicurezza dei GSM
11.2 La crittografia del GSM
11.3 A3 e A8
11.4 L'autenticazione
11.5 Comp128
11.6 Riservatezza delle comunicazioni – A5
11.7 Attacchi al GSM
11.8 Clonazione dei GSM
11.A Bibliografia

12 La Pirateria Satellitare

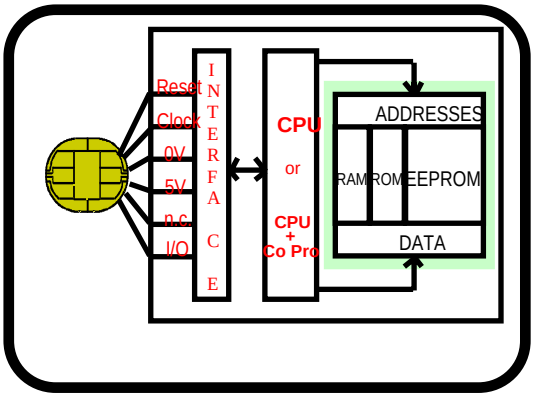
12.1 La trasmissione Satellitare
12.1.1 Sistemi di Codifica
12.1.2 Ricezione e Decodifica
12.1.3 CAM
12.1.4 Smart Card
12.1.5 Schema complete

12.2 Tecniche di Attacco
12.2.1 Analisi dell'assorbimento elettrico
12.3 Strumenti per l'Hacker
12.3.1 Dual Card o Blocker
12.3.2 Titanium Card
12.3.3 Smart Mouse
12.3.4 Season
12.3.5 Wafer Card
12.4 Dall'HW all'emulazione SW
12.4.1 Caso di Studio (NDS – Sky Italia)
12.4.2 Il DREAMBOX
12.A Conclusioni
12.B Bibliografia

0 Descrizione delle Smart Card

Le smart card vengono considerate l'evoluzione delle carte magnetiche. Rispetto a quest'ultime hanno più memoria e sono dotate di una CPU.Una smart card si compone di due parti fondamentali:

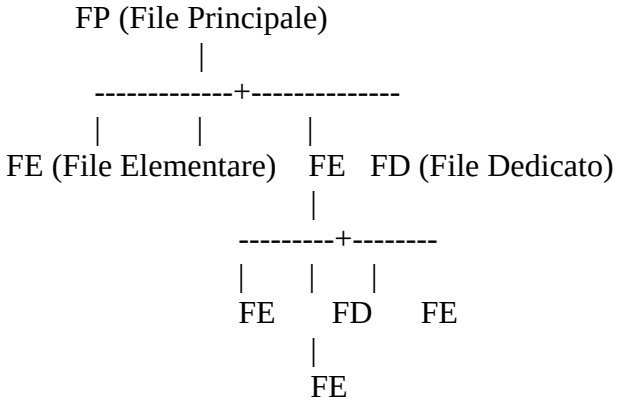
- Il microcircuito
- Il sistema operativo (maschera)



Solitamente la CPU è a 8 bit e la EEPROM mantiene la struttura delle directory e i file riservati relativi a password e chiavi.
Spesso, in aggiunta alla CPU c'è un coprocessore dedicato ad operazioni complesse quali l'uso di algoritmi crittografici a chiave pubblica o per effettuare calcoli matematici pesanti.

La smart card, letteralmente "scheda (o carta) intelligente", è una piccola scheda di plastica, delle dimensioni di una carta di credito, con un microprocessore ed una memoria inclusi al suo interno. Nonostante la sua semplice, insignificante apparenza, ha molteplici usi ed un diffuso utilizzo in applicazioni che spaziano dalle schede telefoniche all'identificazione digitale degli individui.

Queste applicazioni possono essere: certificazione dell'identità del cliente, schede per biblioteche, e-wallet, chiavi per porte, ecc... e per tutte queste applicazioni può essere destinata una sola scheda. Le smart card detengono questi dati all'interno di file diversi e, come si leggerà, questi dati sono visibili ai programmi dipendentemente dal sistema operativo presente nella scheda. Questi file di dati sono collocati in un file system piuttosto simile alla struttura delle directory in Linux.



Il FP (File Principale) può essere considerato come la directory root in cui sono contenute le intestazioni dei file elementari e dedicati. I file dedicati sono simili alle normali directory e quelli elementari ai semplici file di dati. Il PIN è pure contenuto in un FE, ma solo la scheda ha il permesso d'accedere a quel file. Gli attributi dei file propri degli ambienti UNIX sono qui trasformati in condizioni d'accesso. Molte schede possono avere liste di condizioni d'accesso che devono essere soddisfatte prima di accedere ai dati.
Con un file system, condizioni d'accesso, un microcomputer, RAM, ROM, EEPROM, una smart card non è altro che un computer, con il proprio sistema operativo, in grado di stare dentro a un portafoglio.

0.1 Possibili Impieghi

La diffusione di smart card ha avuto tradizionalmente maggior rilevanza in Europa (Francia per il sistema bancario, Germania e Belgio a seguire con carte di credito e di debito), con una crescita sostenuta in funzione dell'adozione generalizzata dei cellulari GSM.
Le recenti leggi che hanno normato l'adozione di questi dispositivi anche a fini identificativi personali, stanno portando al rilascio di carte di identità elettroniche (l'Italia è tra i paesi innovatori in questo campo) ma anche gli Stati Uniti hanno recentemente adottato una legge che recependo in termini molto generali l'esistenza di queste innovazioni tecnologiche, ne codifichi l'impiego per tutte le possibili applicazioni sopra indicate ed altre a venire.
Altri esempi di impiego fin qui definiti sono relativi:

- patenti elettroniche;
- borsellino elettronico (electronic purse);
- tessere di fedeltà, adottate da molte catene di vendita per promuovere le vendite con una politica di incentivazione basata su premi e gratifiche;
- carte telefoniche;
- autentificazione d'accesso e di non-ripudio ad Internet;
- pedaggi elettronici;

- controlli di accesso o afflusso.

Poiché l'aspettativa di diffusione di smart card è di centinaia di milioni di pezzi l'anno, come peraltro avvenuto nel corso degli ultimi 3-4 anni, è evidente che l'affidabilità di questi oggetti costituisce un punto rilevante per la loro generale adozione.
Da studi recenti, si è visto come la difettosità di realizzazione sia ciclicamente critica in fase di primo rilascio per poi assestarsi a livelli di meno di un punto percentuale, mentre le cause di richiesta di duplicati per smarrimento, danneggiamento, alterazione, etc, sono costantemente superiori al 2-3 %.

Ciò comporta che la sensibilizzazione per un loro corretto impiego vada fatta su più fronti:

- un lettore difettoso può danneggiare molte di queste card qualora non lo si rilevi ed isoli in tempo;
- l'utente deve sapere come usarla e come non conservarla al fine di evitarne il danneggiamento;
- va previsto comunque un piano per un rapido subentro di una carta difettosa o smarrita, al fine di stimolare e mantenere una buona confidenza d'uso del mezzo per l'applicazione prevista.

0.2 Applicazioni commerciali

La Smart Card offre notevoli vantaggi per le applicazioni commerciali realizzabili sia in ambienti B2B che B2C. La praticità d'uso e la capacità di aggiornamento delle informazioni rendono la Smart Card una tecnologia particolarmente apprezzata per la connessione tra mondo virtuale e mondo fisico, come in caso di programmi con carta multi/partner.
La carta memorizza ed elabora informazioni, valute e/o applicazioni utilizzabili in vari contesti:

- Operazioni bancarie;
- Fidelizzazione;
- Controllo accessi;
- Custodia dati importanti;
- Identificazione/Riconoscimento;
- Bigliettazione;
- Parcheggi e raccolta pedaggi.

0.3 Applicazioni multiple

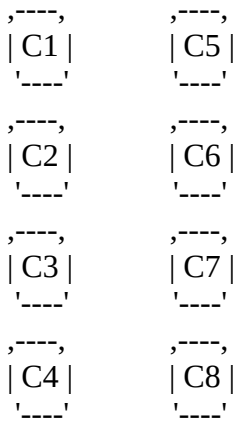
In una Smart Card possono essere memorizzate più applicazioni. La condivisione di più programmi rende più conveniente l'uso del lettore di Smart Card.
Una carta ad applicazioni multiple può supportare contemporaneamente differenti tipi di applicazioni riducendo, pertanto, il numero di carte da portare con sé.

1 Tipi di Smart Card

Per via delle diverse modalità di comunicazione col lettore e le differenti funzionalità incluse, le smart card sono classificate in modi differenti.

1.1 A contatto o senza contatto

Poiché le smart card hanno in esse inclusi dei processori, ne consegue che hanno bisogno di energia per funzionare e di alcuni meccanismi per comunicare, ricevere ed inviare i dati. Alcune smart card hanno placche dorate, ovvero degli insiemi di contatti, in un angolo della scheda. Questo tipo di smart card viene chiamato smart card a contatto (o contact smart card). Le placche sono utilizzate per fornire la necessaria energia e per comunicare attraverso contatti elettrici diretti con il lettore. Quando si inserisce la scheda nel lettore, i contatti di questo si appoggiano alle placche. In base agli standard ISO7816 le connessioni per il PIN sono le seguenti:



C1 : Vcc = 5V
C2 : Reset
C3 : Clock
C4 : RFU
C5 : Gnd
C6 : Vpp
C7 : I/O
C8 : RFU

* I/O : input o output per dati seriali verso i circuiti integrati presenti nella scheda.
* Vpp : input di tensione programmabile (d'utilizzo opzionale per la scheda).
* Gnd : messa a terra (in riferimento alla tensione).
* CLK : segnali di temporizzazione o frequenza (d'utilizzo opzionale per la scheda).
* RST : utilizzato a seconda dei casi da se stesso (per segnali di reset forniti al dispositivo d'interfacciamento) oppure in combinazione con un circuito interno di

controllo del reset (di utilizzo opzionale per la scheda). Se il reset interno è implementato, la fornitura di tensione su Vcc è obbligatoria.
* Vcc : input per la fornitura di tensione (d'utilizzo opzionale per la scheda).

I lettori per le smart card a contatto sono di solito dispositivi separati da collegare alla porta seriale od USB. Esistono tastiere, PC e PDA con inclusi lettori simili a quelli dei telefoni cellulari GSM, anche per mini smart card in stile GSM.

Alcune smart card non hanno connettori sulla propria superficie. La connessione tra il lettore e la scheda viene quindi effettuata via radiofrequenza (RF). Le schede contengono una piccola spira di filo conduttore che viene utilizzata come induttore per fornire energia alla scheda e per comunicare col lettore. Quando la scheda entra nel campo in RF del lettore, una corrente indotta si crea nella spira e viene quindi utilizzata come una sorgente d'energia. Grazie alla modulazione del campo in RF del lettore ed alla corrente indotta nella scheda, la comunicazione ha luogo.
I lettori di smart card di solito si collegano al computer per mezzo della porta seriale od USB. Quando le schede senza contatto (o contactless) non devono essere inserite nel lettore, di solito questo è composto solo da un'interfaccia seriale per il computer e da un'antenna per collegarsi alla scheda. I lettori per smart card senza contatto possono avere o meno un'alloggiamento: la ragione è che alcune smart card possono essere lette fino a 1,5 metri di distanza dal lettore, mentre altre devono essere posizionate a pochi millimetri da esso per poter essere lette con accuratezza.

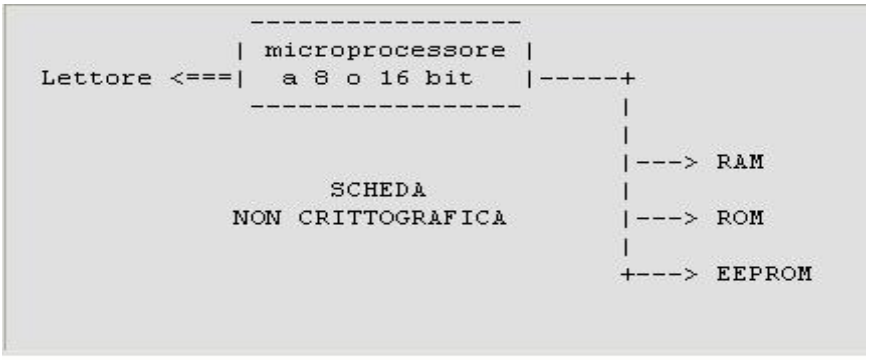
Esiste un ulteriore tipo di smart card, le schede combinate. Una scheda combinata ha un blocco di contatti per la transazione di dati voluminosi, ad esempio le credenziali PKI, ed una spira in filo per la reciproca autenticazione. Le smart card a contatto vengono utilizzate soprattutto per la sicurezza elettronica, mentre quelle senza contatto vengono utilizzate nei trasporti e/o per l'apertura delle porte.

1.2 A memoria o microprocessore

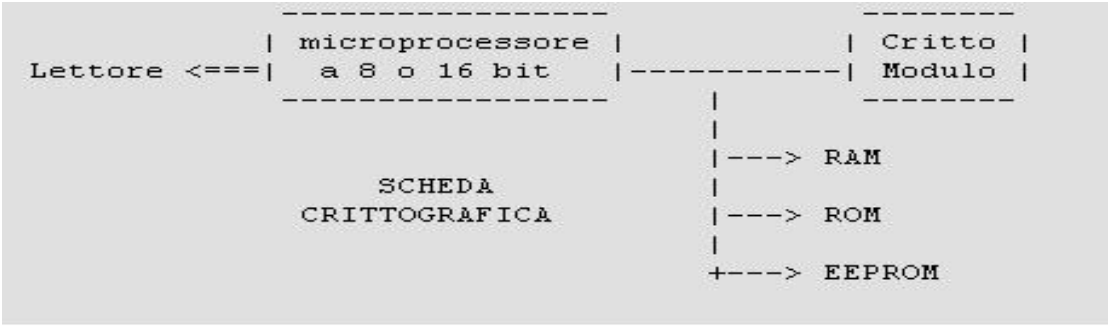
Le smart card più diffuse e meno costose sono schede a memoria. Questo tipo di smart card contiene una memoria permanente EEPROM (Electrically Erasable Programmable Read-Only Memory). Poiché questa è permanente, quando si rimuove la scheda dal lettore e l'energia viene interrotta la scheda salva i dati. Si può immaginare la struttura di una EEPROM come un normale dispositivo d'immagazzinamento dei dati dotato di file system e gestito con un microcontrollore (di solito ad 8 bit). Questo microcontrollore è responsabile dell'accesso ai file e per l'instaurazione della comunicazione. I dati possono essere bloccati con un PIN (Personal Identification Number), la propria parola chiave. I PIN sono normalmente composti da 3 ad 8 numeri che vengono scritti in un file speciale presente nella scheda. Poiché questo tipo di scheda non consente la crittografia, le schede a memoria

vengono utilizzate per contenere credito telefonico, biglietti per il trasporto o denaro elettronico.

Le schede a microprocessore assomigliano molto ai computer che utilizziamo sulla nostre scrivanie. Hanno RAM, ROM e EEPROM con un microprocessore a 8 o 16 bit. Contenuto nella ROM c'è un sistema operativo per gestire il file system presente nella EEPROM e per eseguire le desiderate funzioni nella RAM.



Come si vede dallo schema qui sopra, tutte le comunicazioni sono effettuate attraverso il microprocessore. Non c'è connessione diretta tra la memoria ed i contatti. Il sistema operativo è responsabile della sicurezza dei dati presenti in memoria perché è lui a controllare le condizioni d'accesso.



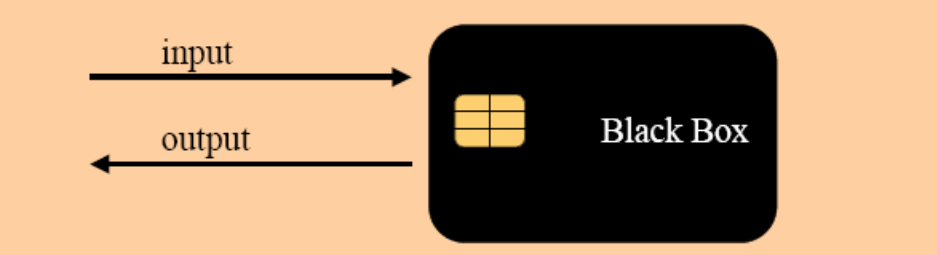
Con l'aggiunta di un crittomodulo, la nostra smart card può ora gestire i complessi calcoli matematici relativi al PKI. Poiché la frequenza interna dei microcontrolli è compresa tra 3 e 5 MHz, si ha la necessità di aggiungere un componente che acceleri le funzioni crittografiche. Le schede crittografiche sono più costose di quelle non crittografiche, così come le schede a microprocessore lo sono più di quelle a memoria.

La scelta della scheda corretta dipende dalle proprie applicazioni.

2 Struttura Logica

Una smart card può essere vista come una scatola nera:

- riceve un input
- processa l'input
- restituisce un output
- I dati non sono mai direttamente raggiungibili
- Il flusso di dati è bidirezionale



3 Il Sistema Operativo

Il Sistema operativo è mascherato nella memoria ROM e sovrintende alle seguenti funzioni:

- Gestione del protocollo di comunicazione;
- Gestione del protocollo logico (APDU);
- Gestione dello SmartCard File System;
- Sicurezza:
  - Sicurezza fisica (protezione degli "oggetti di sicurezza" contenuti nella SmartCard);
  - Sicurezza logica (criteri di accesso ai file ed agli oggetti di sicurezza).

La nuova moda nei sistemi operativi per smart card è il JavaCard Operatine System. Il JavaCard OS è stato sviluppato da Sun Microsystem e quindi promosso al JavaCard Forum. Il JavaCard OS è popolare poiché rendere indipendenti i programmatori rispetto all'architettura e applicazioni pensate per il JavaCard OS possono essere utilizzate da qualsiasi produttore di smart card che supportino JavaCard OS.

La maggior parte delle smart card usano oggi i loro specifici OS per le sottostanti comunicazioni e funzioni. Per poter dare un reale supporto alle applicazioni i sistemi operativi per smart card vanno ben oltre le semplici funzioni indicate dagli standard ISO7816. Conseguenza di ciò è che il porting delle applicazioni sviluppate per un

produttore verso un altro produttore di smart card diventa un lavoro particolarmente complesso. Un altro vantaggio del JavaCard OS è che permette il concetto del caricamento posticipato delle applicazioni. Ciò permette di aggiornare le applicazioni delle smart card dopo la consegna della scheda all'utente finale.
L'importanza sta nel fatto che l'utilizzo di una smart card è legato all'esecuzione di un'applicazione specifica, necessità che però successivamente può cambiare e rendere necessaria l'esecuzione di un maggior numero di applicazioni.

Un altro sistema operativo per smart card è MULTOS (Multi-application Operating System). Come il nome stesso suggerisce, MULTOS può anch'egli supportare più applicazioni. MULTOS è tuttavia stato disegnato specificatamente per necessità d'elevata sicurezza ed in molte nazioni ha conseguito la certificazion "ITSec E6 High".

Anche Microsoft sta interessandosi alle smart card con Smart Card for Windows.

I citati sistemi operativi possono essere quindi considerati come API dal lato scheda per sviluppare cardlets o piccoli programmi in grado d'essere eseguiti sulla scheda. Esistono inoltre API dal lato lettore come OpenCard Framework e GlobalPlatform.

4 Sicurezza delle Smart Card

Le tecniche di sicurezza impiegate nella progettazione delle smart card e nelle procedure di autenticazione/trasmissione di questi dati verso i terminali d'interfaccia riguardano essenzialmente quattro settori:

- integrità dei dati
- autenticazione
- irriproducibilità
- riservatezza

4.1 Integrità dei dati

Per integrità dei dati si intende la corretta trasmissione dei dati tra sorgente (smart card) e destinatario (terminale di servizio) senza nessun tipo di alterazione dell'informazione. L'integrità dei dati viene garantita da sofisticate tecniche crittografiche chiamate *check digits*, ossia controllo delle cifre (è una procedura numerica che consente di determinare se un certo insieme di valori numerici, i bit memorizzati nella card, sono stati alterati o meno).
Si utilizzano per questo scopo procedure chiamate *hashing* che numericamente vincolano a un insieme stabilito di valori numerici un altro insieme di valori calcolati sulla base dei primi (una sorta di targa numerica). Se anche un singolo bit dell'insieme

informativo viene alterato, il valore di hash viene modificato. Esistono diversi algoritmi di hash utilizzati per garantire l'integrità dei dati, in particolare si utilizzano:

- SHA-1 Secure Hash Algorithm: produce una targa di 160 bit per un insieme informativo di valori numerici di 2^{64} bit di lunghezza al massimo.
- MD5 Message Digest 5: produce una targa di 128 bit e quindi 16 caratteri.

4.2 Autenticazione

E' una tecnica simile a quella di hashing precedentemente introdotta che consente di stabilire se un insieme informativo proviene realmente da una fonte originaria. In sostanza si aggiungono dei dati, una sorta di firma digitale, all'insieme informativo da trasmettere per scongiurare eventuali manomissioni. Questa firma digitale non è altro che una scansione particolare del contenuto informativo dell'insieme dei dati, che può essere utilizzata dal ricevente come verifica dell'autenticità. Tramite un valore numerico derivato da una funzione hash con l'aggiunta di una chiave privata, è possibile determinare matematicamente l'autenticità di un documento. Anche per questa tecnica esistono vari algoritmi, tra i più diffusi ci sono:

- DSA Digital Segnature Algorithm: utilizza una chiave privata di lunghezza variabile tra 512 e 1024 bit.
- RSA: utilizza chiavi private fino 2048 bit.

In pratica queste tecniche di autenticazione utilizzano algoritmi asimmetrici con chiavi pubbliche e private. L'autenticazione si basa sulla chiave pubblica del mittente per verificare che il messaggio sia realmente stato inviato dalla giusta sorgente. Una verifica dell'algoritmo di testing consente di determinare o meno l'autenticazione.

4.3 Irriproducibilità

Bisogna in qualche modo garantire che questa "firma digitale" non possa essere copiata per consentire l'invio di messaggi fasulli apparentemente autentici.
Questo problema è uno degli aspetti cruciali della sicurezza in ambito elettronico. Chiunque con un minimo di attrezzatura è in grado di copiare il contenuto informativo di un dispositivo digitale e la copia risultante sarà indistinguibile dall'originale, questo perché, essendo digitalizzata, l'informazione è rappresentata con una serie di bit che, una volta copiata, rappresenta fedelmente la stessa informazione della sorgente.

4.4 Riservatezza

L'obiettivo è quello di evitare che un intruso possa catturare e decifrare le operazioni interpretando di conseguenza il contenuto informativo della smart card.

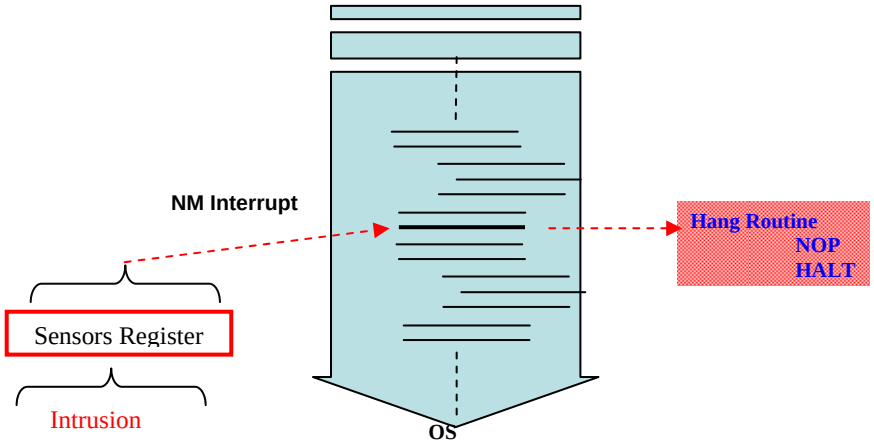
5 Sicurezza Fisica

La sicurezza fisica è l'insieme delle contromisure messe in atto per proteggere le informazioni da attacchi condotti tramite:

- **l'utilizzo improprio dell'interfaccia elettrica**
- **azioni fisiche volte a guadagnare il controllo diretto del microprocessore**
- **analisi dell'assorbimento elettrico**

Contromisure principali

- Sensori che rilevano la marginatura della tensione di alimentazione
- Sensori che rilevano la marginatura del clock
- Sensori di temperatura di esercizio
- Sensori ottici



6 Sicurezza Logica

La sicurezza logica controlla l'accesso alle informazioni contenute nella smart card tramite:

- codici personali di accesso alle informazioni (PIN);
- processi di autenticazione realizzati con tecniche crittografiche simmetriche o asimmetriche;

- funzioni che consentono di rendere non modificabili ed accessibili in sola lettura alcuni dati;
- funzioni che consentono di rendere non esportabili gli oggetti di sicurezza (chiavi e codici di accesso).

6.1 Gli Oggetti della Sicurezza

PIN

- Consente di verificare il possesso della della Smart Card, ad esso possono essere associate condizioni di accesso ai file e condizioni di utilizzo degli oggetti di sicurezza
- Possono essere definiti più PIN

Chiavi crittografiche simmetriche ed asimmetriche

- Consentono di realizzare processi di autenticazione
- Ai processi di autenticazione possono essere vincolate le condizioni di accesso ai file
- Le chiavi possono essere usate anche per produrre crittografia da utilizzare all'esterno della Smart Card (p.e. Firma Digitale)

6.2 Smart Card come Motori Crittografici

Le Smart Card supportano algoritmi simmetrici (DES e 3 DES) e algoritmi asimmetrici (RSA) che utilizzano gli oggetti di sicurezza tramite comandi APDU

- Gli oggetti di sicurezza sono utilizzabili se è settato l'ambiente di sicurezza tramite il comando MSE (Manage Security Environment)
- La crittografia è sviluppata per mezzo del comando PSO xxx (Perform Security Operation) dove xxx vale:
    - CDS per Digital Signature e MAC;
    - ENC per cifratura simmetrica e asimmetrica;
    - DEC per decifratura simmetrica ed asimmetrica.

Di seguito elenchiamo, per completezza, i vari standard crittografici delle smart card:

- PCSC
- Muscle
- Datacard

- Muelbauher
- PKCS#11
- CSP
- ASN1
- CardOS – Siemens
- CNS
- Firma digitale
- Secure Messaging

6.3 Librerie Crittografiche

Le *PKCS#11* sono delle *Application Programming Interface* (API) che interfacciano dispositivi crittografici ovvero dispositivi che memorizzano chiavi e sviluppano calcoli crittografici.

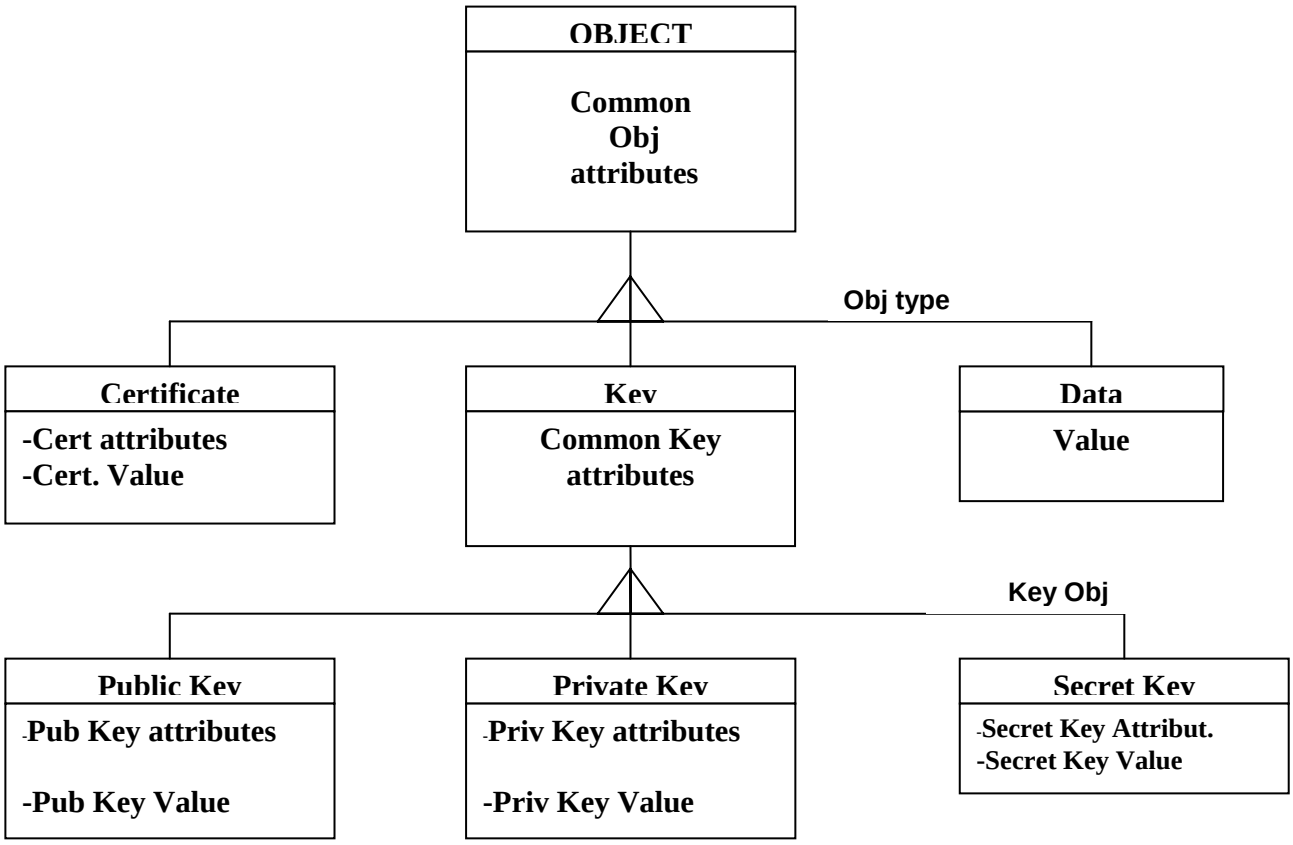
- Forniscono una interfaccia standard che prescinde dal dispositivo crittografico per cui sono state sviluppate.
- Rendono le applicazioni in cui la crittografia è trattata con queste API largamente indipendenti dai dispositivi.

- Vincolano all'utilizzo del dispositivo crittografico per cui sono state sviluppate ovvero non consentono a Smart Card di differenti fornitori di poter operare sulla stessa piattaforma applicativa.

Gli scopi delle Cryptoki in base allo standard:
Obiettivo primario: un'interfaccia di programmazione di basso livello che astrae i dettagli dei dispositivi e presenta alle applicazioni un comune modello del dispositivo crittografico detto *cryptographic token*.
Obiettivo secondario: ottenere risorse condivise. Un singolo dispositivo può essere condiviso tra varie applicazioni e un'applicazione può interfacciare più di un dispositivo alla volta.

Il **"Token"** delle Cryptoki:

- È la rappresentazione a oggetti dei dati e delle quantità di sicurezza contenute nel dispositivo crittografico
    - Gli oggetti sono definiti dagli attributi (template)
- Contiene la definizione dei meccanismi crittografici supportati dal dispositivo



Funzioni delle PKCS#11

- Funzioni per la gestione dei lettori e delle SmarCard:

C_GetSlotList
C_GetSlotInfo
C_GetTokenInfo
C_GetMechanismList
C_GetMechanismInfo
C_InitToken
C_InitPIN
C_SetPIN

- Funzioni per la gestione della sessione:

C_OpenSession
C_CloseSession
C_CloseAllSession
C_GetSessionInfo
C_Login
C_Logout

- Key Management:

C_GenerateKey
C_GenerateKeyPair
C_WrapKey
C_UnwrapKey

- Funzioni di firma e verifica firma:

C_SignInit
C_Sign
C_SignUpdate
C_SignFinal
C_VerifyInit
C_Verify
C_VerifyUpdate
C_VerifyFinal

- Funzioni di Message Digesting:

C_DigestInit
C_Digest
C_DigestUpdate
C_DigestFinal

Identificazione e Autenticazione in Rete

- Identificazione : lo "Username" è sostituito da un certificato digitale. L'Utente è caratterizzato dal suo Codice Fiscale.

- Autenticazione : la "password" è sostituita da un crittogramma prodotto per mezzo della chiave privata di autenticazione contenuta nella smart card.

- Il colloquio tra client e server è caratterizzato da scambi di dati caratterizzati da procedure riferite al cosiddetto Challenge/Response.

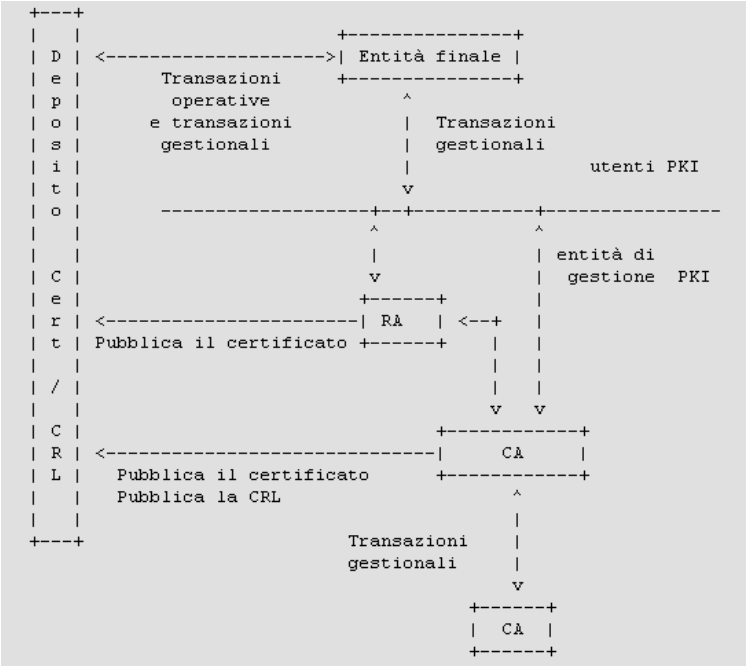
- Quando il colloquio è in modalità "web browsing" viene utilizzato il protocollo TLS/SSL (Transport Layer Security/Secure Socket Layer)

- Garantiscono oltre che l'autenticazione del titolare anche l'autenticazione del server.

6.4 Rapporto tra PKI e Smart Card

La **Public-key infrastructure (PKI)** è una infrastruttura di sicurezza costituita da protocolli e servizi, aderenti a standard, per il supporto di applicazioni basati su crittografia a chiave pubblica.
La PKI consente di realizzare le principali funzioni di sicurezza delle transazioni commerciali. La **CA** è preposta alla generazione dei certificati digitali delle chiavi pubbliche dei partecipanti alla PKI.

Come già sappiamo, le smart card sono luoghi sicuri su cui collocare dati sensibili, quali soldi ed identità personale. E se l'argomento è l'identità personale dobbiamo parlare di PKI, Public Key Infrastructure, e smart card. Si immagini di lavorare in un'azienda con molte filiali e succursali. In queste grandi aziende gli impiegati hanno frequentemente permesso d'accedere in diversi luoghi fisici. Inoltre, si può accedere ai server aziendali per varie mansioni quali inviare posta elettronica, aggiornare le pagine web ed accedere ai database aziendali. Si pensi, una password per ogni server ed una chiave per ogni porta e dei soldi in portafoglio per acquistare cibo o bevande nel ristorante più vicino. In realtà, si potrebbe utilizzare una smart card. Se s'utilizza una scheda a microprocessore ed il sistema operativo della scheda oppure le cardlet Java lo consentono, si potrebbe in effetti utilizzare un'unica scheda per tutto questo. Affinché questo scenario sia fattibile, l'azienda deve disporre di una propria CA, Certificate Authority. Lo schema seguente mostra una semplice struttura PKI, come descritto nell'RFC 2459.



- entità finale: utente dei certificati PKI e/o il sistema utente finale che è il soggetto del certificato;

- RA: registration authority, ovvero un sistema opzionale cui una CA delega certe funzioni gestionali; (in alcune implementazioni, dove tu registri te stesso nel sistema)
- CA: certification authority; (la propria chiave pubblica può essere resa pubblica quando ci si registra oppure può essere resa automaticamente pubblica, firmata e quindi il certificato pubblico viene consegnato dalla CA)
- deposito: un sistema o collezione di sistemi distribuiti che conserva i certificati e le CRL, Certificate Revocation Lists, e che è mezzo per la distribuzione di questi certificati e CRL alle entità finali.

In realtà, questa è solo una visione semplificata delle entità PKI. L'impiegato o l'entità finale si riferisce semplicemente alla CA od alla RA per ottenerne un certificato. Un certificato è solo una chiave pubblica digitalmente firmata con la chiave privata dell'ente rilasciante, la CA. Se firmato con la chiave privata della CA, tutti coloro che ripongono fiducia in essa danno automaticamente fiducia all'entità finale. La propria ID digitale è servita, bisogna solo scrivere la propria ID digitale e la chiave privata nella smart card, meglio ancora se s'utilizzano le nuove smart card, rilasciate con funzioni incluse che generano chiavi pubbliche e private all'interno della scheda, il che significa che la tua chiava privata non è esportata verso alcun luogo.
Le schede di nuova generazione sono in grado di utilizzare funzioni PKI che non richiedono d'esportare la chiave privata verso l'applicazione utilizzata. Ad esempio, quando si vuole mandare una mail firmata il programma di posta elettronica prima genera una hash del documento che si ha appena scritto e poi instaura la comunicazione con la scheda. L'applicazione quindi invia il valore dell'hash alla scheda, che provvede a firmare dentro se stessa tale valore con la chiave privata contenuta nella scheda medesima. In questo modo, la chiave privata non viene mai esportata verso l'ambiente pubblico, ovvero il computer.
Inoltre, quando si accede ad un proprio account remoto si può utilizzare un client ssh, la shell sicura. Un metodo di autenticazione per il protocollo ssh2 è descritto nella man page di OpenSSH. Il principale proposito di tal metodo è l'effettiva identificazione della persona che tenta d'accedere all'account e quindi l'instaurazione di una connessione tra gli host, qualora l'utente venisse accettato. In teoria, solo l'utente può conoscere la propria chiave privata. Sebbene la chiave privata sia leggibile solo dal proprietario, questo può essere un rischio di sicurezza, ma se la chiave privata viene memorizzata all'interno di una smart card si può ottenere una maggiore sicurezza. Naturalmente può capitare di perdere una smart card, ma a questo punto interviene un ulteriore argomento di sicurezza, il PIN. In generale, si può dire che la sicurezza delle smart card ha due origini, una che si sa ed una che si possiede.
SSH non è l'unica applicazione per cui si possono utilizzare le smart card. Transazioni monetarie in rete, autenticazione presso siti cui ci si connette ed altre applicazioni possono essere svolte grazie alle smart card. Il sistema è sempre più o meno lo

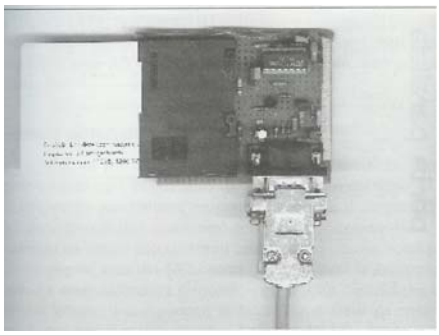
stesso: l'identificazione viene verificata attraverso la chiave privata ed una sessione sicura viene avviata con le chiavi; a questo punto emergono specifiche e diverse componenti delle applicazioni, così come son state pensate e realizzate dal fornitore dell'applicazione. In alcuni casi le transazioni monetarie vengono effettuate all'interno della smart card, ma con altre applicazioni ad essa viene solo richiesto il numero di conto corrente bancario. Ci possono essere poi ulteriori metodologie.
È possibile trovare sul mercato serrature elettroniche che dialogano con una smart card. PKI può supportare, in aggiunta alla reciproca autenticazione di scheda e lettore, il conteggio degli accessi nello stabile. Si può utilizzare la semplice e reciproca autenticazione, oppure la serratura può effettuare una richiesta ad un server locale che contiene i dati degli utenti e verificare se all'utente è concesso di oltrepassare la porta e, sia che l'accesso sia concesso oppure rifiutato, il server tiene traccia dei tentativi d'accesso.
Man mano che l'integrazione delle smart card con il mondo PKI procederà, molte nuove applicazioni verranno create, soprattutto riguardanti vari aspetti della sicurezza oppure per semplificare la vita dell'utenza.

7 Lettori di Smart Card

Esistono in circolazione diversi lettori di smart card. Di seguito parleremo solo di alcuni tra i più famosi nel circuito degli hacker, e quindi interessanti perché autocostruiti, solamente trasparenti nell'utilizzo e soprattutto facili da realizzare anche dal punto di vista economico.

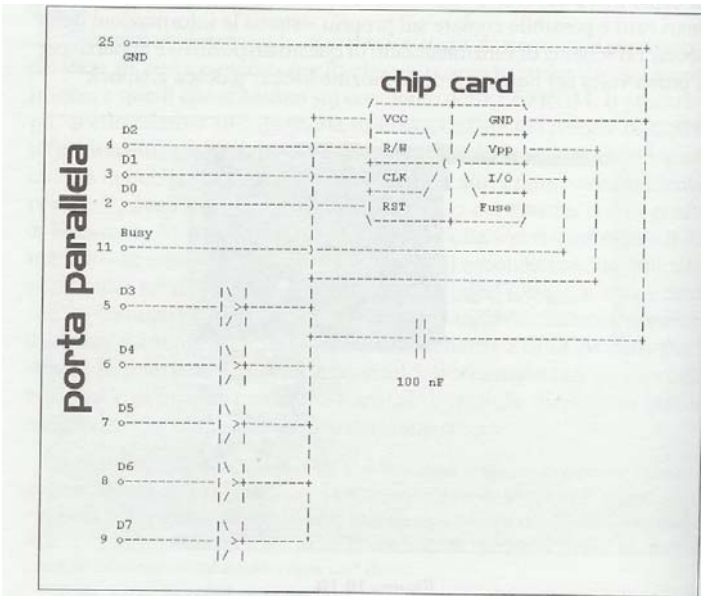
7.1 Dumb mouse

Si tratta di un semplice letture universale di smart card. Di facile realizzazione elettronica e utilizzo, il Dumb mouse consente di leggere il contenuto informativo del chip presente in una smart card, collegandola alla porta seriale di un comune personal computer. Con un semplicissimo programma in grado di eseguire il Dump (la copia fisica dei valori della memoria) dei dati nella EEPROM della smart card è possibile copiare sul proprio sistema le informazioni della stessa. Lo schema di funzionamento di questo dispositivo è apparso per la prima volta nel n°2 della Fantine Hacker tedesca Klaphek.

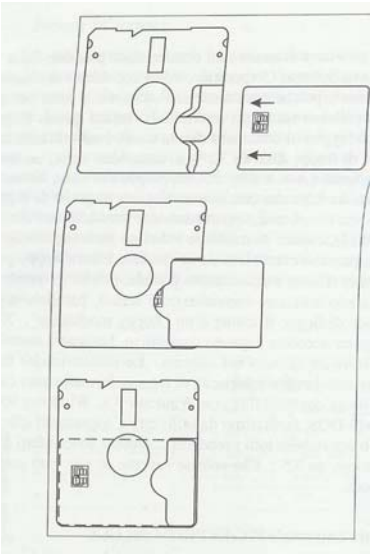


7.2 Simple PC Reader

A differenza del Dumb mouse, questo lettore, ancora più facile da implementare, consente di leggere il contenuto informativo di una smart card utilizzando la comunicazione parallela di un personal computer. I dati vengono letti quasi direttamente dalle porte di comunicazione del chip della card, semplicemente utilizzando componenti comuni, come condensatori e diodi 1n4148, adoperati per il collegamento con i pin della porta parallela di un computer. Lo stesso schema elettronico e il principio di funzionamento di questo semplicissimo lettore di smart card sono apparsi per la prima volta nella rivista Electronics designe nel mese di febbraio 1997.



7.3 Smarty



Si tratta di un lettore di card commerciale prodotto dalla Fischer International Systems Corporation.
Questo dispositivo consente di leggere il contenuto di una smart card un comune lettore di floppy disk da 3,5". Smarty non è altro che un dispositivo delle dimensioni di un dischetto da 3,5", che contiene un circuito in grado di leggere il contenuto di una smart card, opportunamente introdotta nel contenitore, capace di trasferire i dati su tecnologia magnetica, in modo che possano essere lette da un comune lettore floppy per personal computer. L'idea è sicuramente geniale, poiché in questo modo non è necessario utilizzare comunicazioni seriali, parallele o peggio ancora schede dedicate; il lettore è un "floppy

modificato" naturalmente, per poter accedere a questo dispositivo, bisognerà installare un opportuno software nel sistema.

7.4 Software universale PIC/EEPROM del CCC

Si tratta di software universale per l'interfaccia, tra personal computer e smart card di qualsiasi tipo. Sviluppato dal Chos Computer Club, questo pacchetto di programmi consente di leggere il contenuto informativo di una smart card generica appoggiandosi a livello di hardware a un lettore autocostruito interfacciato tramite porta parallela.

8 Algoritmo DSA (cenni)

Nel 1994 il NIST, l'ente federale USA, nel quadro degli standard DSS (Digital Signature Standard) ha approvato l'algoritmo DSA come standard federale per la firma digitale (DSA non è utilizzabile per la crittazione). Usa un algoritmo inventato da David Kravitz e derivato da quello di Schnorr.

Generazione delle chiavi.
La configurazione dell'algoritmo DSA richiede di fissare alcuni parametri e quindi di generare le chiavi segreta e pubblica:
Si fissa un numero primo m da usare nelle operazioni di resto modulo, con $2^{511}<m<2^{512}$.
Si fissa un numero Q, divisore primo di m-1, con $2^{159}<Q<2^{160}$.
Si fissa un numero G, con $0<G<m-1$.
Si sceglie una chiave segreta S_A, con $0<S_A<Q$.
La chiave pubblica si calcola come $P_A=G^{S}{}_A$.

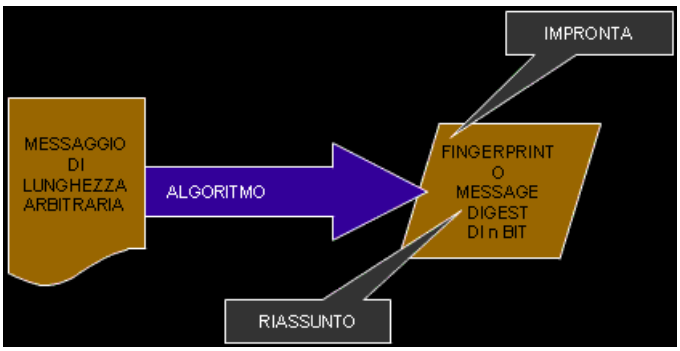
Generazione della firma digitale.
Siccome nelle operazioni di modulo previste da questo algoritmo si usano moduli diversi nelle diverse fasi del calcolo, a differenza di quanto ho scritto finora qui indicherò esplicitamente il modulo impiegato come pedice della coppia di parentesi quadrate. Per la firma del messaggio M si procede così:
Scegliere un numero h, con $0<h<Q$.
Calcolare $u=[[G^h]_m]_Q$.
Determinare il valore di v risolvendo la relazione $D(M) = [S_A\ u + h\ v]_Q$, dove D() è la funzione digest scelta.
La firma digitale di M è la coppia di numeri (u,v).

Verifica della firma digitale.
Determinare w tale che $w\ v = [1]_Q$.
Calcolare $i = [D(M)\ w]_Q$.
Calcolare $l = [u\ w]_Q$.

Calcolare $t = [\,[G^{i}\,P_A]_m\,]_Q$.
Verificare che sia $t = u$.
DSA è stato criticato dalla comunità crittografica per varie ragioni: la verifica della firma, una operazione senz'altro più comune della sua generazione, è particolarmente inefficiente ed è più lenta dalla generazione della firma stessa; l'iter di approvazione di questo standard da parte del NIST è stato piuttosto arbitrario e con un ampio contributo da parte di NSA; esistono alcuni particolari numeri primi che, se usati dal programma per la generazione della firma, possono indebolire l'algoritmo e, sebbene alcuni di questi numeri sono stati individuati, è plausibile che ve ne siano altri ancora da scoprire; il range dei parametri ammessi sembra piuttosto arbitrario.

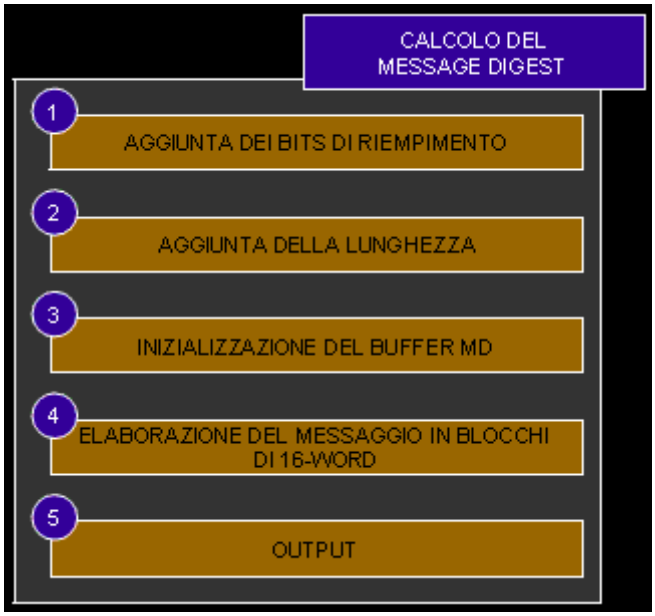
9 Algoritmo MD5 (cenni)

L'algoritmo MD5 genera un'impronta, chiamata anche fingerprint o message digest, della lunghezza di 128 bits, di un messaggio di lunghezza arbitraria.



L'algoritmo, appartenente alla RSA Data Security, Inc. è stato sviluppato da R. Rivest nel 1991.

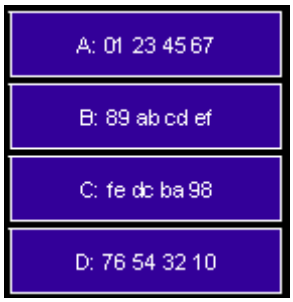
L'algoritmo è suddiviso in cinque fasi principali:



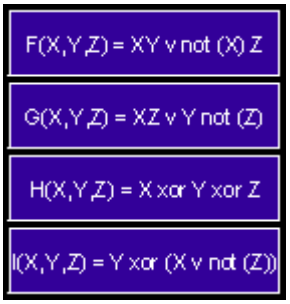
Aggiunta bits di riempimento: il messaggio viene sempre esteso (padding) così che la sua lunghezza in bits sia congruente a 448 mod 512. Il primo bit di estensione è sempre un '1' seguito da una serie di '0' mentre il numero di bits di estensione va da un minimo di 1 ad un massimo di 512.

Aggiunta della lunghezza: viene aggiunta una rappresentazione a 64-bit della lunghezza del messaggio (b) prima del riempimento. Se la lunghezza era maggiore a 2^64 vengono utilizzati solo i 64 bits inferiori di b e le due word a 32-bit risultanti vengono accodate, seguendo la rappresentazione vista in precedenza, con la word più bassa per prima. Il messaggio ottenuto ha una lunghezza multipla di 512 bits (in pratica 16 words da 32-bit).

Inizializzazione del buffer MD (initial variable/chaining variable): si tratta di un buffer di quattro word (A, B, C, D) a 32-bit aventi questi valori esadecimali di inizializzazione (la prima word per prima):



Elaborazione del messaggio (compression function): vengono definite quattro funzioni ausiliare che ricevono in ingresso tre words da 32-bit e producono in uscita una sola word a 32-bit:

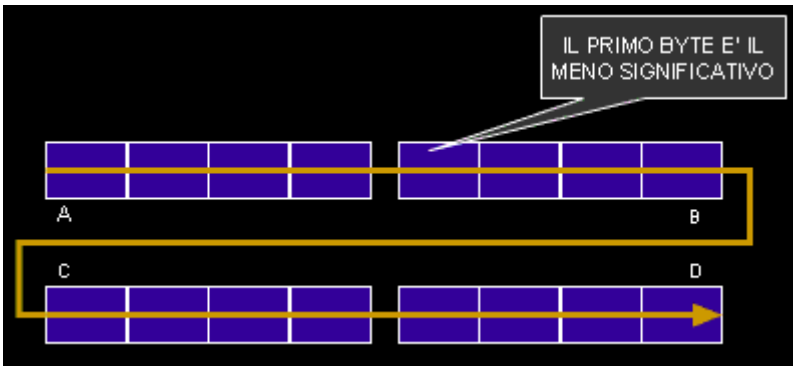


Per ogni bit le funzioni applicano la condizione che, se è vero X passano ad Y, altrimenti a Z, senza introdurre una propria logica ma, seguendo quella dei singoli bits.
La funzione H produce, mediante un operazione di XOR binario, la 'parità' dei bit ingresso. In questo passaggio viene anche utilizza una tabella T di 64 elementi T[1… 64] così da avere per ogni T[i] un valore equivalente alla parte intera di 4294967296 volte abs(sin(i)), con i espresso in radianti.
Ogni blocco da 16-word viene elaborato seguendo questo algoritmo:

```
/* Elabora ogni blocco da 16 word. */
For i = 0 to N/16-1 do

/* Copia il blocco i dentro X. */
For j = 0 to 15 do
     Set X[j] to M[i*16+j]
end /* del ciclo j */

/* Salva A come AA, B come BB, C come CC, e D come DD. */
AA = A
BB = B
CC = C
DD = D

/* Passaggio 1. */
/* [abcd k s i] indica l'operazione:
a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
/* Effettua le seguenti 16 operazioni. */

[ABCD  0  7  1]  [DABC  1 12  2]  [CDAB  2 17  3]  [BCDA  3 22  4]
[ABCD  4  7  5]  [DABC  5 12  6]  [CDAB  6 17  7]  [BCDA  7 22  8]
[ABCD  8  7  9]  [DABC  9 12 10]  [CDAB 10 17 11]  [BCDA 11 22 12]
[ABCD 12  7 13]  [DABC 13 12 14]  [CDAB 14 17 15]  [BCDA 15 22 16]

/* Passaggio 2. */
/* [abcd k s i] indica l'operazione:
a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
/* Effettua le seguenti 16 operazioni. */

[ABCD  1  5 17]  [DABC  6  9 18]  [CDAB 11 14 19]  [BCDA  0  20 20]
[ABCD  5  5 21]  [DABC 10  9 22]  [CDAB 15 14 23]  [BCDA  4  20 24]
[ABCD  9  5 25]  [DABC 14  9 26]  [CDAB  3 14 27]  [BCDA  8  20 28]
[ABCD 13  5 29]  [DABC  2  9 30]  [CDAB  7 14 31]  [BCDA 12  20 32]

/* Passaggio 3. */
/* [abcd k s t] indica l'operazione:
a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
/* Effettua le seguenti 16 operazioni. */

[ABCD  5  4 33]  [DABC  8 11 34]  [CDAB 11 16 35]  [BCDA 14 23 36]
[ABCD  1  4 37]  [DABC  4 11 38]  [CDAB  7 16 39]  [BCDA 10 23 40]
[ABCD 13  4 41]  [DABC  0 11 42]  [CDAB  3 16 43]  [BCDA  6 23 44]
[ABCD  9  4 45]  [DABC 12 11 46]  [CDAB 15 16 47]  [BCDA  2 23 48]
```

```
/* Passaggio 4. */
/* [abcd k s t] indica l'operazione:
a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
/* Effettua le seguenti 16 operazioni. */

[ABCD  0  6  49]  [DABC  7 10  50]  [CDAB 14 15 51]  [BCDA  5  21 52]
[ABCD 12  6  53]  [DABC  3 10  54]  [CDAB 10 15 55]  [BCDA  1  21 56]
[ABCD  8  6  57]  [DABC 15 10  58]  [CDAB  6 15 59]  [BCDA 13  21 60]
[ABCD  4  6  61]  [DABC 11 10  62]  [CDAB  2 15 63]  [BCDA  9  21 64]

/* Quindi esegue le seguenti addizioni. (Ad ognuno dei quattro registri viene aggiunto il
valore che aveva prima dell'inizio del processo) */

A = A + AA
B = B + BB
C = C + CC
D = D + DD

end /* fine del ciclo  i */
```

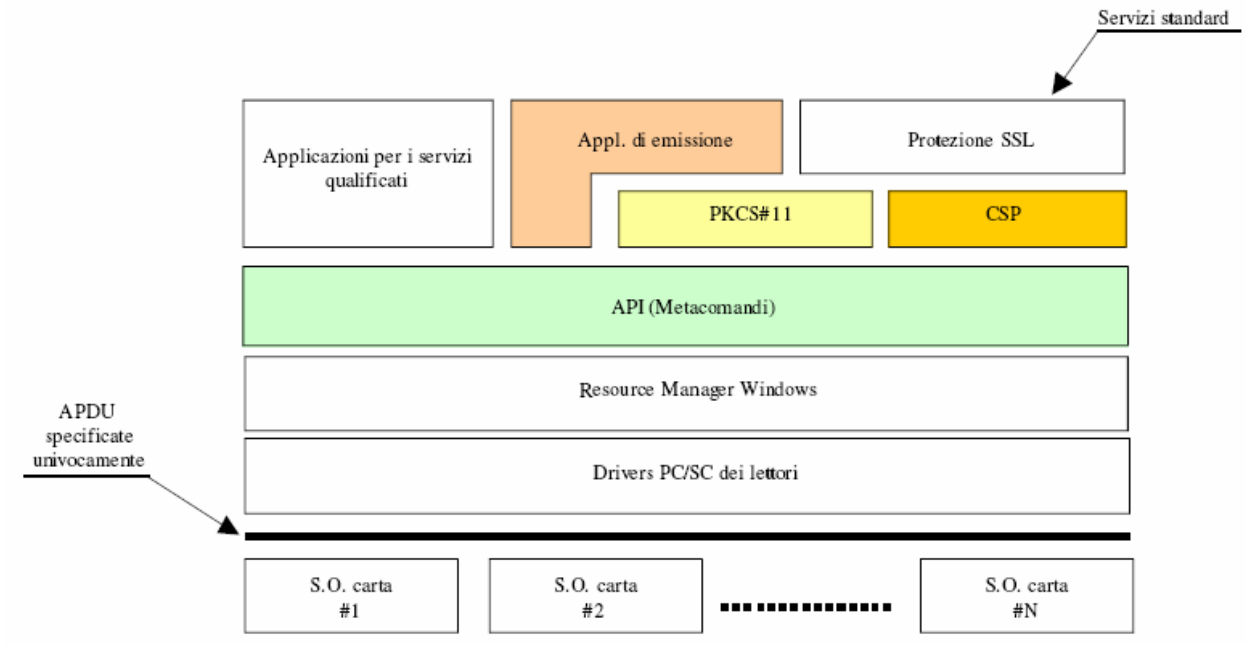
Output: Il message digest è ottenuto partendo dal byte meno significativo di A seguito da quelli di B, C, e terminato con il byte più significativo di D.



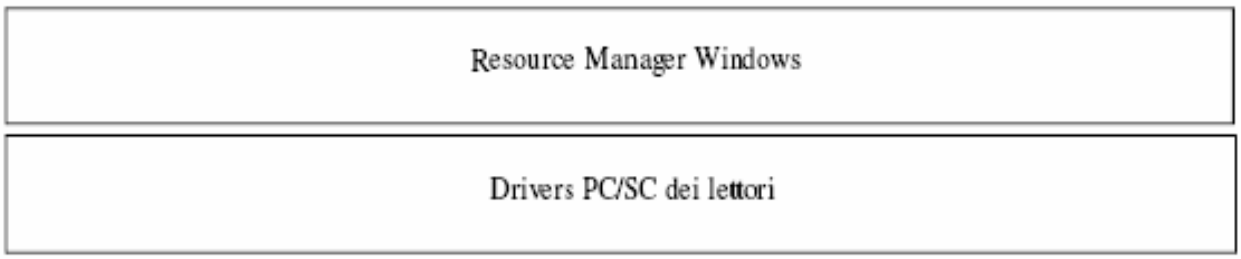
10 CARTA D'IDENTITA' ELETTRONICA (CIE)

10.1 L'architettura

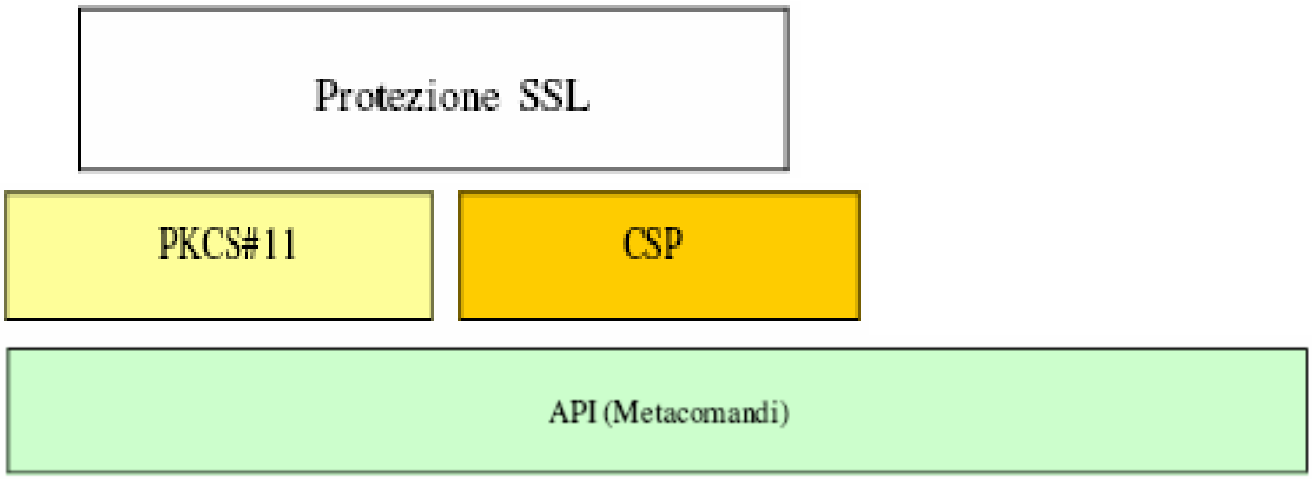
- La CIE è una carta a microprocessore in grado di ospitare applicazioni che possono essere sviluppate anche da terze parti1.
- L'architettura di riferimento della CIE è stata progettata per garantire l'indipendenza delle applicazioni dai sistemi operativi delle carte e permettere la realizzazione di servizi qualificati che sfruttino al meglio le caratteristiche di versatilità e sicurezza delle carte a microprocessore.



Il Resource Manager di Windows viene utilizzato per consentire di prescindere rispetto alle specificità dei lettori di chip, che devono essere però equipaggiati di driver PC/SC.



Lo strato intermedio PKCS#11 (o in ambiente Microsoft il CSP) può essere utilizzato dagli attuali browser per funzioni native di sicurezza che sfruttano il protocollo SSL V3.



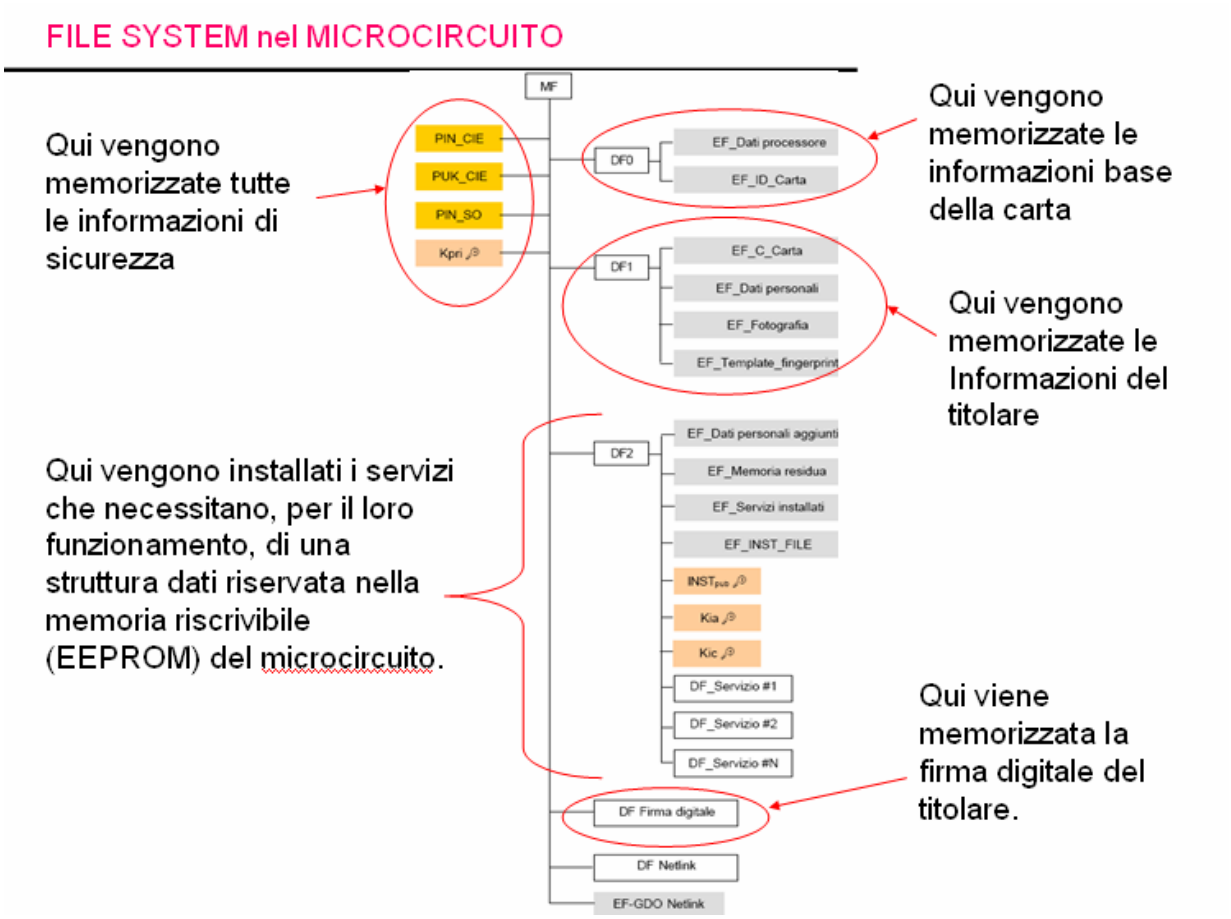
Le API (cioè i metacomandi) rappresentano l'interfaccia tra le applicazioni e la carta a microprocessore. Esse sono standard, sono pubblicate dal Ministero dell'Interno e possono essere utilizzate per realizzare applicazioni che sfruttano le risorse delle carte a microprocessore, prescindendo dal tipo di carta (purché aderente alle specifiche pubblicate).

10.2 Metacomandi CIE

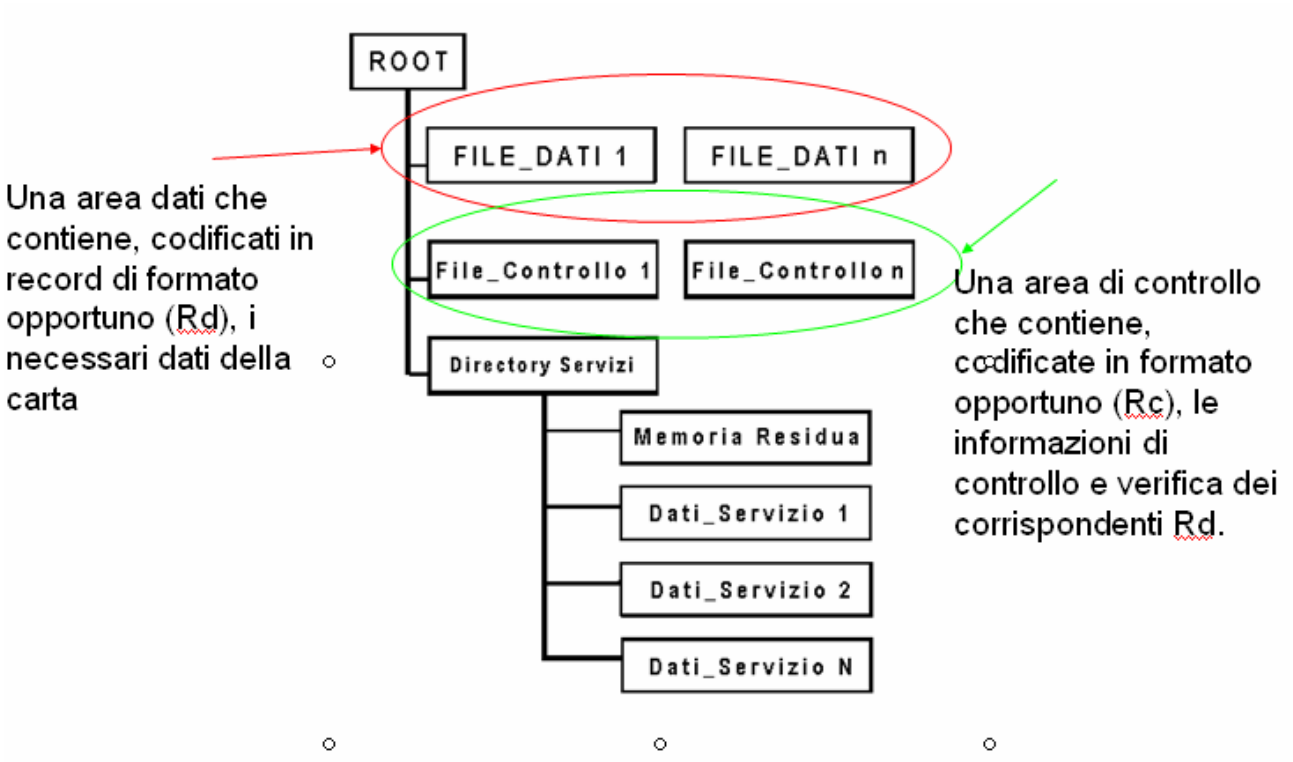
```
#define MAX_DATA 0x100
struct CIE_DATA
{
char strNome[MAX_DATA];
char strCognome[MAX_DATA];
char strSesso[MAX_DATA];
char strStatura[MAX_DATA];
char strComuneEmittente[MAX_DATA];
char strComuneResidenza[MAX_DATA];
char strComuneNascita[MAX_DATA];
char strIndirizzo[MAX_DATA];
```

```
char strDataNascita[MAX_DATA];
char strCodiceFiscale[MAX_DATA];
char strDataEmissione[MAX_DATA];
char strDataScadenza[MAX_DATA];
char strCittadinanza[MAX_DATA];
char strAttoNascita[MAX_DATA];
char strStatoEsteroNascita[MAX_DATA];
bool bEspatrio;
};

#define _CIE_PIN_INVALID
#define _CIE_PIN_BLOCKED
```

- Operazioni sul PIN
- Operazioni sul PUK
- Operazione crittografica di firma
  - Input: Oggetto DigestInfo e sua lunghezza;
  - Output: Dato firmato e sua lunghezza.
  - *DWORD CIE_Sign(BYTE* pbtDigestInfo, BYTE btDigestInfoLen, BYTE* pbtSignedData, DWORD& dwSignedDataLen);*
- Operazione di hashing
  - Input: Dato in chiaro e sua lunghezza;
  - Output: Hash SHA-1 del dato e sua lunghezza.
  - *DWORD CIE_HashDataSHA1(BYTE* pbtData, DWORD dwDataLen, BYTE* pbtHash, BYTE& btHashLen);*



10.3 Struttura delle informazioni sulla banda ottica



10.4 Sicurezza del supporto fisico

- **Elementi di sicurezza grafici e di stampa**
    - motivi antiscanner ed antifotocopiatura a colori;
    - stampa con effetto rainbow (a sfumatura di colore graduale e progressiva);
    - embedded hologram (incisione grafica su banda laser);

- **Numerazione di serie**
    - inserito sia sulla carta che nella banda ottica e nel microprocessore

- **Applicazione di elementi Optical Variable Device (OVD)**
    - Sul retro del documento, nella fase di produzione, è applicato a caldo un ologramma di sicurezza.

10.5 Affidabilità dei dati

- **Laser su banda ottica**
    - I dati vengono memorizzati permanentemente sulla banda laser (sistema WORM) in formato digitale e letti/scritti con appositi apparati, detti lettori/scrittori;
    - Nella banda laser, è attivo un metodo di identificazione e correzione d'errore che garantisce la ricostruzione delle informazioni digitali eventualmente perse per cause accidentali.

- **Microcircuito**
    - Livello fisico
        - ✓ La protezione a livello fisico è gestita dal produttore del chip che provvede a mascherare sulla carta, in maniera indelebile, il sistema operativo proteggendolo mediante una chiave segreta di cui egli solo è a conoscenza.
    - Livello logico.
        - ✓ Il livello logico è invece gestito sia dall'entità che inizializza la CIE che dall'ente che la personalizza.

- **Sicurezza del circuito**

  - La migliore garanzia contro tentativi di falsificazioni e utilizzo di carte rubate si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione della CIE.

- **Sicurezza degli accessi ai dati**

  - I dati sono prima cifrati per mezzo di un algoritmo simmetrico di provata robustezza (ad es. 3DES) con una chiave di lunghezza non inferiore a 128 bit (generata in modalità casuale);

  - Quest'ultima, prima di essere distrutta, viene a sua volta cifrata sia con la chiave pubblica della Questura che con quella del Comune e memorizzata assieme all'informazione.

- **Sicurezza della carta**

  - I rischi di furto e falsificazione delle carte d'identità, con l'adozione del modello elettronico, sono notevolmente ridotti.

  - La banda ottica rappresenta l'elemento centrale della sicurezza:
    - non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili.

- **Sicurezza della carta**

  - In ogni caso esistono le protezioni inserite nell'hardware di scrittura, in dotazione esclusivamente a E ed IPZS, e di ogni operazione effettuata dal funzionario autorizzato elettronicamente si tiene traccia presso SSCE.

  - Inoltre non essendo la banda laser modificabile attraverso campi magnetici, calore (l00°), campi elettrici, virus informatici, il suo contenuto è inattaccabile.

  - Inoltre tutte le informazioni sensibili, tanto sul chip che sulla banda ottica, sono garantite contro l'alterazione, perché "firmate" digitalmente.

10.6 Algoritmi utilizzati

- Gli algoritmi asimmetrici comunemente impiegati dalle Smart Card ed idonei per realizzare la autenticazione :

    - l'algoritmo RSA;
    - l'algoritmo DSA.

- Si preferisce l'RSA per la possibilità di avere una lunghezza di chiave doppia rispetto a quella del DSA

10.A Bibliografia

- http://www.cnipa.gov.it/site/_contentfiles/01378200/1378274_SeminarioCNIPASmartCard(01102004).ppt
- http://www.cnipa.gov.it/site/_files/SmartCardAvanzato18062004.ppt
- http://www.akron.it/akronstore/index.php?cPath=5_6
- http://www.amagri.it/Crittologia/Crittografia/Algoritmi_crittografici/MD5/algoritmo_md5.htm
- http://it.tldp.org/HOWTO/Smart-Card-HOWTO/smartpki.html
- http://it.tldp.org/HOWTO/Smart-Card-HOWTO/classification.html
- http://it.tldp.org/HOWTO/Smart-Card-HOWTO/smartcardintro.html
- http://www.icosaedro.it/crittografia/chiavi-simmetriche.html#algoritmodsadigitalsignaturealgorithml
- http://www.cwi.it/showPage.php?id=12426&template=articoli
- http://www.cartaidentita.it/cie/reader/index.html
- http://www.fontesarda.it/urg/dm2000_c.htm#art04

Sicurezza delle Reti Cellulari

11 Il telefono e la crittografia

Negli ultimi anni l'utilizzo dei telefoni cellulari è aumentato notevolmente.
La domanda che viene quasi spontanea è come sono implementate le tecniche di sicurezza delle comunicazioni?
Innanzi tutto sappiamo che le comuni e normali conversazioni su telefoni tradizionali non sono protette in termini di sicurezza, in quanto non vengono utilizzati sistemi di cifratura della conversazione poiché gli standard attuali delle compagnie telefoniche non li prevedono.
In realtà, esistono però sistemi chiamati "scrambler" che consentono di mascherare e quindi cifrare le normali conversazioni telefoniche.

Inoltre con l'avvento delle linee digitali è divenuto molto più semplice intercettare le telefonate senza avere più bisogno di istallare fisicamente congegni e morsetti su terminali sparsi sulla rete.
Grazie ad un personal computer, una chiave di accesso e conoscendo i protocolli di manutenzione delle reti telefoniche un malintenzionato potrebbe senza troppi problemi introdursi nelle centraline di una compagnia telefonica e registrare tranquillamente qualsiasi conversazione.
Le chiavi di accesso sono facilmente identificabili attraverso tecniche di social engineering ("faccia tosta") o di trashing ("rovistare nei rifiuti") oppure avere accesso all'informazione tramite corruzione, sembrano situazioni da film ma in realtà sono più reali di quanto si creda.
Per quanto riguarda le comunicazioni cellulari, le prime erano basate su tecnologia analogica (TACS) e quindi erano facilmente intercettabili grazie a semplici radio in grado di coprire la gamma di frequenza di 900 Mhz. Attraverso questi comuni radio scanner è inoltre possibile intercettare informazioni utili sul canale di controllo delle comunicazioni e ricostruire persino la posizione dell'utente nella cella territoriale. Quindi la crittografia a livello di TACS/ETACS non esiste.

Con l'avvento del GSM e quindi delle tecniche digitali sono stati introdotti standard crittografici per la protezione/autenticazione delle conversazioni telefoniche. Tutte

le moderne tecniche di crittografia si basano su algoritmi applicati a informazioni digitali, quindi la voce per essere protetta deve essere digitalizzata.

11.1 La sicurezza dei GSM

Nella telefonia digitale la sicurezza è implementata per mezzo di un meccanismo di stratificazione delle procedure di autenticazione, di riservatezza dei dati dell'utente e soprattutto della riservatezza delle comunicazioni e dei segnali di controllo.
Ogni volta che utilizziamo un cellulare GSM la nostra chiamata viene digitalizzata, cifrata e inviata alla centrale ricevente più vicina. Nella stazione ricevente la chiamata verrà decifrata e inviata in chiaro al numero telefonico corrispondente. Quindi tutte le comunicazioni via etere sono criptate, ma nessuno ci assicura che un malintenzionato non intercetti le telefonate a terra.

11.2 La crittografia del GSM

Il sistema di comunicazione GSM si avvale di alcuni algoritmi crittografici di tipo simmetrico, chiamati A3, A5 e A8. Questi algoritmi vengono utilizzati per le procedure di autenticazione e mascheramento dei messaggi. In particolare gli algoritmi A3 e A8 sono utilizzati in fase di autenticazione della chiamata e della trasmissione, mentre l'algoritmo A5 per la cifratura della comunicazione e quindi questo è l'algoritmo che un malintenzionato dovrebbe effettivamente violare per poter decifrare la comunicazione. Questo algoritmo essendo così importante è quindi riservato.
Comunque rimane importantissima anche l'autenticazione in quanto oltre a proteggere il contenuto della mia telefonata è importante garantire che effettivamente sia io a chiamare e non un malintenzionato che abbia clonato il mio GSM.

L'abbonato è identificato univocamente dal codice IMSI che, unitamente alla chiave personale di autenticazione Ki, costituiscono le credenziali di identificazione. L'innovazione particolare è che le procedure di autenticazione e crittografia al fine di garantire maggiore sicurezza e protezione nel sistema si esplicano in modo che queste informazioni non vengano trasmesse sul canale radio.

11.3 A3 e A8

L'algoritmo A3 è l'algoritmo di Autenticazione dell'MS
L'algoritmo A8 è l'algoritmo di generazione della chiave di sessione Kc

Questi algoritmi sono anche chiamati nel gergo delle funzioni hash "key-dependent" (dipendenti da una chiave) e "one-way" (cioè è particolarmente difficile calcolarne l'inversa).

Ma che cosa è in sostanza una funzione hash?
Una funzione hash è una trasformazione che dato un ingresso m arbitrario, di dimensione variabile, restituisce in uscita una stringa di lunghezza fissa chiamata "valore hash h" (h = H(m)).
Sostanzialmente una funzione hash è una trasformazione che lega una targa, rappresentata da un numero, ad un insieme di valori numerici che rappresentano l'informazione da autenticare, nel nostro caso dati binari relativi alla comunicazione cellulare.
Questi algoritmi quindi sono usati per garantire l'autenticità della fonte di trasmissione di un segnale.

Ma le funzioni hash e questi algoritmi simmetrici come operano realmente nelle comunicazioni GSM?

La sicurezza nel GSM è basata sostanzialmente su 3 punti:

1. La scheda smart card inserita fisicamente nel cellulare, SIM (Subscriber Identity Module)
2. Il cellulare (Mobile Equipment)
3. La rete GSM, BTS (base transceiver station)

Nella SIM sono memorizzate le seguenti informazioni:

- il codice IMSI
- la chiave personale di autenticazione Ki
- l'algoritmo A8 che genera la chiave temporanea Kc
- l'algoritmo A3 di autenticazione
- il codice PIN personale

Nell' ME è invece memorizzato l'algoritmo A5 di cifratura per i dati relativi alla comunicazione
Nelle BTS sono memorizzati l'algoritmo A5 per la decifrazione dei messaggi e la chiave temporanea Kc.

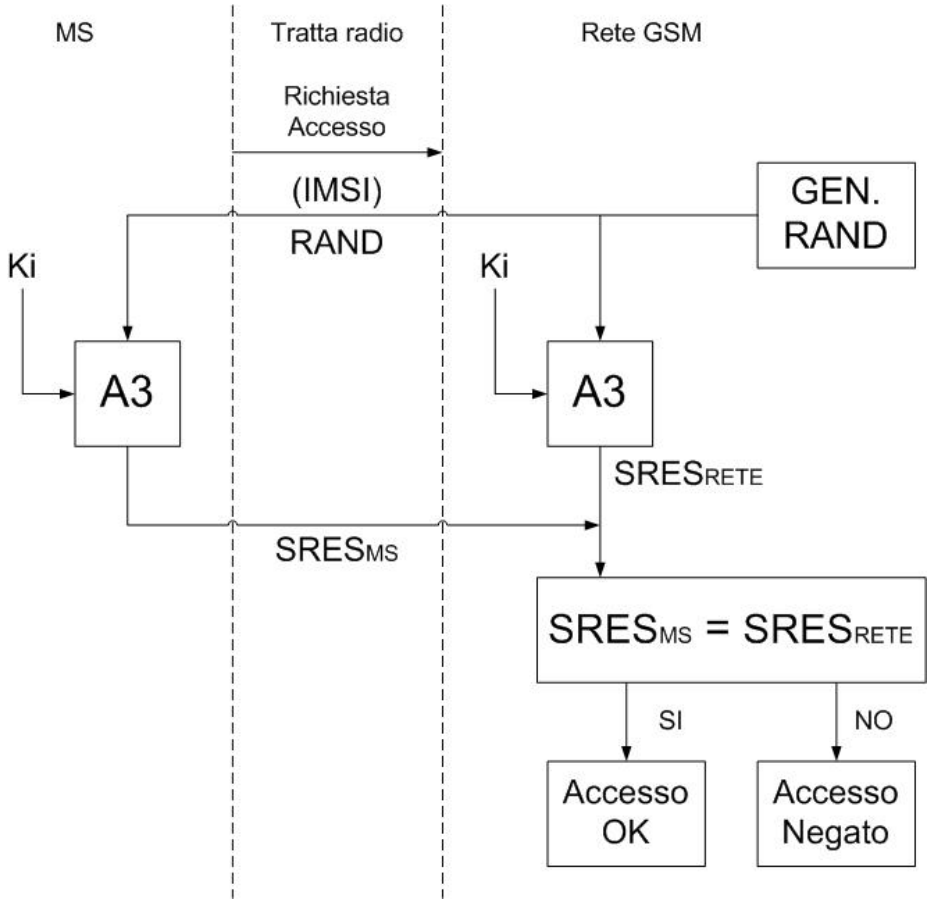
Il processo legato ad una chiamata telefonica si compone di due fasi:

1. la fase di autenticazione
2. la fase di comunicazione

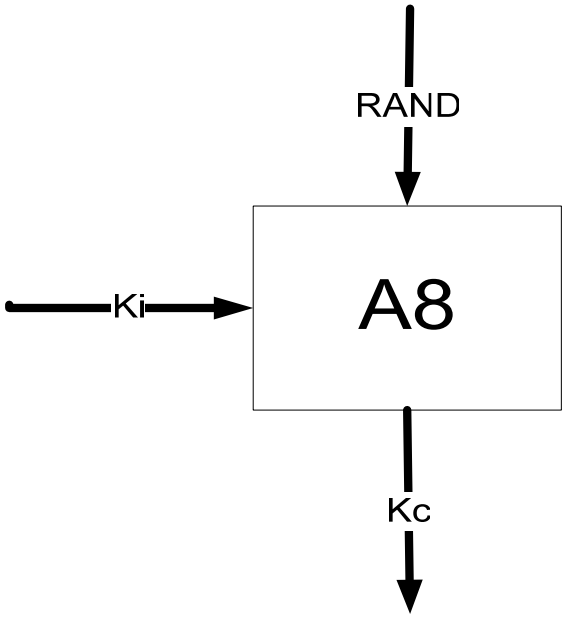
11.4 L'autenticazione

Avviene tra i moduli SIM e il centro di autenticazione AuC (Authentication Center) presente nella stazione BTS. Ogni qualvolta utilizziamo il cellulare per ricevere o effettuare chiamate, per aggiornare la posizione della stazione mobile o quando vengono eseguite le operazioni di attivazione, disattivazione, interrogazione dei

servizi supplementari viene attivata la procedura di autenticazione. L'autenticazione avviene tramite una procedura detta challenge-response, ossia a ogni richiesta di autenticazione da parte della stazione mobile l'AuC risponde generando un numero casuale di 128 bit (RAND) come sfida (challenge). La stazione mobile dopo aver ricevuto questo codice (RAND) lo utilizza come input per l'algoritmo A3 con la chiave personale Ki, il risultato che viene chiamato SRES, di 32 bit, viene spedito (response) all' AuC per l'autenticazione. L'AuC per mezzo del RAND e della stessa chiave Ki genera a sua volta il SRES, infine confronta il suo risultato con il SRES ricevuto dalla stazione mobile; se i valori coincidono la procedura di autenticazione è andata a buon fine altrimenti viene negato l'accesso alla rete GSM.
L'AuC è in possesso della chiave Ki dell'utente sin dall'inizio poiché i dati dell'utente sono memorizzati nell'HLR (Home Location Register), cioè in un database apposito relativo alla rete di appartenenza dell'utente.
In questo modo le chiavi Ki non sono trasmesse lungo il canale essendo in possesso sia della SIM che della AuC, e quindi la sicurezza è garantita.



A questo punto, se l'autenticazione è andata a buon fine, la stazione base e la stazione mobile calcolano la chiave Kc che servirà per cifrare la comunicazione. La chiave Kc viene calcolata per mezzo dell'algoritmo A8 fornendogli in input il RAND e la chiave Ki.



La scelta di generare un numero casuale (RAND) è dovuta al fatto che se tale stringa non fosse generata, il valore SRES trasmesso dalla MS alla BTS sarebbe sempre lo stesso: si potrebbe dunque effettuare un attacco a ripetizione.

All'inizio della fase di autenticazione l'MS utilizza, per farsi identificare, il codice IMSI dell'utente. Per evitare che questo codice continui a viaggiare nel canale, appena eseguita l'autenticazione dell'utente viene utilizzato per il resto delle operazioni un codice temporaneo TMSI per garantire così maggiore sicurezza. Questo codice è temporaneo e varia in base alla locazione in cui si trova l'utente mobile.

11.5 Comp128

Invece di utilizzare due algoritmi distinti, A3 ed A8, la maggior parte degli operatori GSM utilizza un unico algoritmo, chiamato COMP128.

L'algoritmo consiste nel creare un'array di 96 bit dei quali:

1. I primi 32 rappresentano SRES
2. Gli altri 64 (di cui gli ultimi 10 sono sempre posti uguali a zero) rappresentano la chiave kc

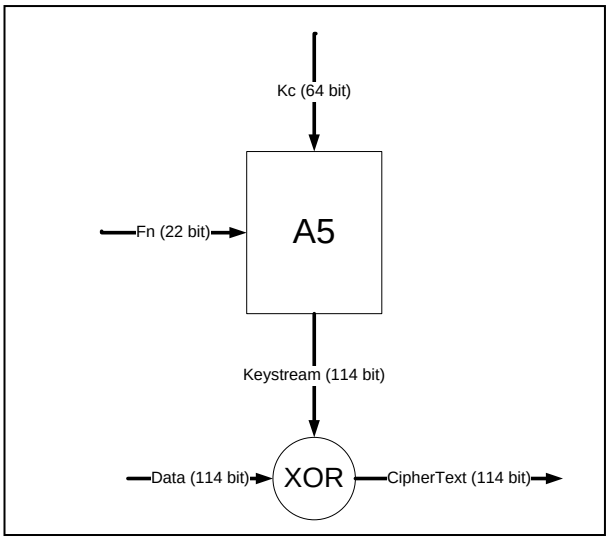
Il COMP128 e' considerato però un algoritmo debole ed infatti è stato violato tramite un attacco di tipo fisico alla SIM Card.

In generale anche gli altri algoritmi utilizzati dal GSM sono deboli, proprio perché gli ultimi 10 bit della chiave di sessione kc sono posti uguali a zero. Quindi lo spazio delle chiavi si riduce da 2^{64} a 2^{54} .

Tutto questo è stato favorito dai diversi governi in sede di standarizzazione del protocollo per rendere possibile l'intercettazione ed il controllo delle chiamate.

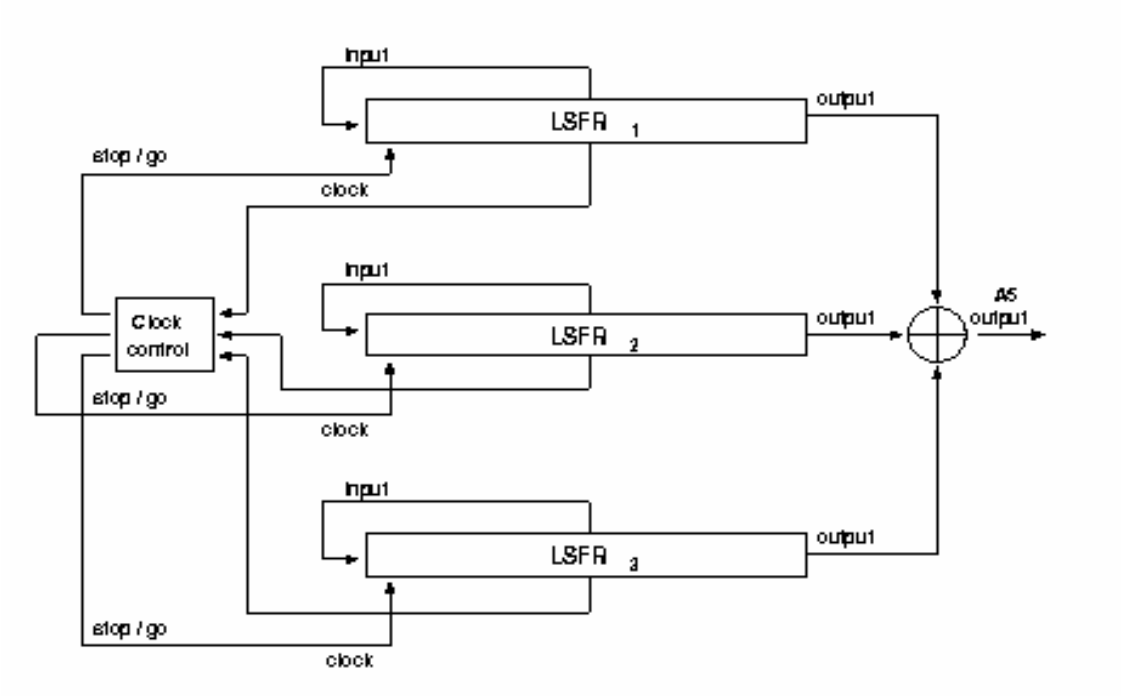
11.6 Riservatezza delle comunicazioni – A5

Come detto precedentemente viene effettuata tramite l'algoritmo A5 (Algoritmo di cifratura).
L'algoritmo A5 è un codificatore di tipo "stream chiper" ossia un algoritmo che opera su singoli bit cifrandoli uno alla volta. Questo algoritmo usa una chiave di cifratura Kc di 64 bit e il numero della trama TDMA di 22 bit per produrre una sequenza di 114 bit (keystream) che viene utilizzata per crittografare i 114 bit significativi di ogni burst (i due blocchi di 57 bit) attraverso un exclusive or XOR. La chiave Kc è diversa per ogni comunicazione anche dello stesso utente poiché è una chiave temporanea utilizzata per l'identificazione della stazione base con il dispositivo mobile e quindi viene generata ad ogni comunicazione in modo tale da garantire la riservatezza e la non tracciabilità del chiamante.

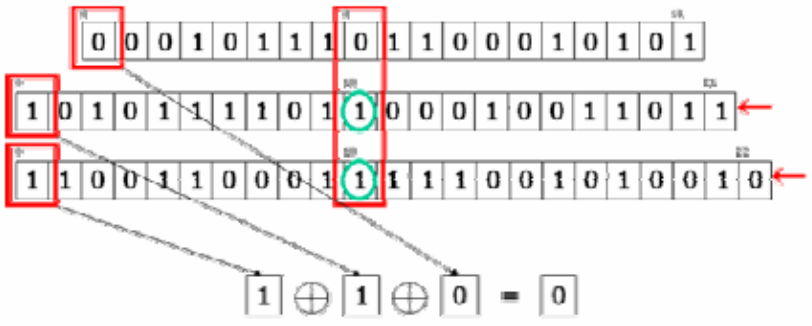


L'algoritmo consiste in tre registri a scorrimento a retroazione lineare rispettivamente di 19, 22 e 23 bit, sincronizzati. La sincronizzazione (clock control) di ciascun registro è una funzione limitata dei bit centrali dei 3 registri la somma dei tre registri è 64 e infatti la chiave di cifratura di 64 bit è utilizzata per inizializzarli ad ogni sessione.

Dopo il caricamento dei bit della chiave di sessione ciascuno dei 22 bit del numero di frame viene messo in XOR con i tre valori di feedback dei registri stessi.
Durante il caricamento di ciascun bit del numero di frame, vengono shiftati i registri il cui bit centrale concorda con il bit di maggioranza.



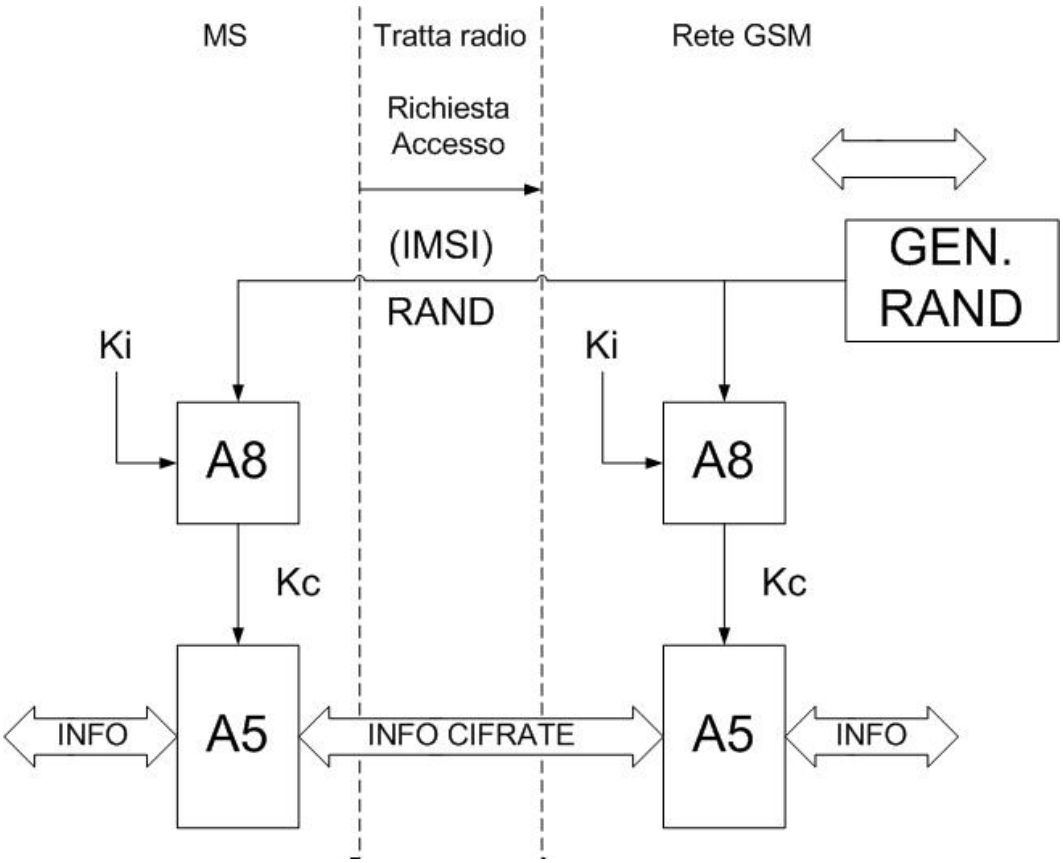
I 3 registri sono sincronizzati in base al bit centrale di ognuno.
Ciascun registro viene shiftato se il suo bit centrale concorda con il valore di maggioranza dei bit centrali dei tre registri garantendo quindi che ad ogni iterazione vengono shiftati almeno due registri.
Il bit della keystream è calcolato come XOR del bit meno significativo dei 3 registri.



Dopo che i registri sono stati inizializzati con la chiave di sessione Kc ed il numero del frame corrente:

- i primi 100 bit di output della keystream vengono scartati allo scopo di distribuire i bit del numero di frame in modo casuale nei tre LFSR;
- vengono prodotti 114 bit di output della keystream, che vengono utilizzati per cifrare il frame da MS a BTS;
- vengono scartati altri 100 bit di output dell keystream per nascondere la relazione tra i primi 114 bit ed i succesivi 114 bit della keystream;
- vengono prodotti 114 bit di output della keystream, che vengono utilizzati per decifrare il frame successivo ricevuto dalla BTS.

Questo algoritmo viene utilizzato per la cifratura/decifratura dei messaggi tramite l'utilizzo di una chiave Kc generata dall'algoritmo A8 mediante l'utilizzo del numero casuale RAND e della chiave personale Ki. In questo modo anche in questo caso non c'è scambio della chiave nel canale e quindi anche se si dovesse riuscire a superare la procedura di autenticazione non si potrebbe comunicare a causa della chiave Kc. In pratica Ki e KC costituiscono dei lucchetti impenetrabili concatenati l'uno con l'altro. Inoltre Kc dipendendo da Rand viene ad ogni comunicazione cambiata. Proprio perché generata tramite RAND la chiave Kc è diversa per ogni comunicazione anche dello stesso utente. Così si garantisce la riservatezza e la non tracciabilità del chiamante.



Intercettare e decrittare al volo una telefonata non è un'operazione difficile per chi abbia a disposizione mezzi e risorse, che comunque risultano costose.
In realtà ascoltare le nostre conversazioni è molto più semplice poiché l'architettura GSM prevede, come detto in precedenza, che la conversazione sia cifrata dal telefono alla cella, la BTS, ma da questo punto in poi il traffico viaggia in chiaro. Lo scopo di questo meccanismo così debole è appunto il poter rendere accessibile il contenuto della rete ad operatori e autorità competenti.

Inoltre come ben sappiamo uno dei problemi più ricorrenti in ambito di comunicazione cellulare è la clonazione dei nostri GSM.

11.7 Attacchi al GSM

Gli attacchi al GSM sono di diversi tipi:

- Attacchi diretti agli algoritmi di cifratura
- Attacchi diretti alla SIM Card
- Attacchi alla rete GSM

Per quanto riguarda la prima tipologia di attacco, questa può essere realizzata mediante diverse tecniche:

- Attacco Brute-Force :
  - In real-time non è possibile ma si può memorizzare il frame tra la MS e la BTS e lanciare l'attacco in un secondo momento con una complessità in tempo pari a 2^{54} operazioni.

- Attacco Divide-and-Conquer (Known Plaintext) :
  - Attacco di tipo known-plaintext. L'attaccante tenta di determinare lo stato iniziale degli LFSR da una sequenza di keystream conosciuta. Egli ha bisogno di conoscere solo 64 bit consecutivi della keystream che vengono calcolati dalle coppie testo in chiaro-testo cifrato a lui note. L'attacco è implementato indovinando il contenuto dei due LFSR più corti e computando il terzo LFSR dalla keystream conosciuta mediante la risoluzione di equazioni lineari appropriate. Questo attacco richiederebbe in media 2^{40} tentativi, nell'ipotesi in cui gli shift dei primi due registri non fossero dipendenti dal terzo registro.

La seconda tipologia di attacchi è quella che mira a carpire informazioni dalla SIM Card stessa. Anche in questo caso l'attacco può essere effettuato con tecniche diverse:

- Attacco Logico:

    - L'attacco via etere è basato sul fatto che la MS deve rispondere ad ogni challange inviatagli dalla BTS. Un malintenzionato potrebbe impersonare la BTS inviando alla MS delle challenge per scoprire la chiave segreta mediante le sue risposte.

- Attacco fisico:

    - Richiede l'accesso fisico alla SIM ed è di tipo **chosen-challenge**.
    - La chiave segreta può essere dedotta dalle risposte SRES mediante crittoanalisi differenziale.

- Rottura dell'algoritmo Comp128:

    - Attacco Chosen-Challeng:
        - Si formulano alla SIM una serie di richieste tratte da uno specifico insieme di input. La SIM applica l'algoritmo alla propria chiave segreta e all'insieme di input scelti, restituendone la risposta. L'analisi delle risposte porta alla comprensione ed alla rottura dell'algoritmo, con la conseguente individuazione della chiave.

    - Partitioning Attack:
        - Monitorando i side-channels, come ad esempio il consumo di energia o l'emanazione elettromagnetica (EM), un hacker potrebbe ottenere in pochi minuti le chiavi segrete contenute nelle SIM card con tutte le informazioni sull'identità dell'utente.

Gli attacchi alla rete GSM sono riconducibili agli attacchi visti precedentemente in quanto i concetti sono gli stessi ma vengono applicati in condizioni diverse:

- Accesso ai segnali della rete :

    - Se l'attaccante può accedere ai segnali degli operatori della rete sarà capace di ascoltare ogni cosa che viene trasmessa. La rete di segnalazione SS7 utilizzata dagli operatori della rete GSM è completamente insicura se l'attaccante ne guadagna l'accesso diretto. L'attaccante potrebbe provare ad accedere all'HLR di una particolare rete. Accedere ai segnali della rete non è molto difficile. Sebbene le BTS siano di solito connesse alle BSC attraverso un cavo, alcune di esse sono

connesse alle BSC per mezzo di microonde. Sarebbe relativamente facile accedere a tale link con il giusto tipo di attrezzatura. Non è inoltre esclusa la possibilità di accedere al cavo di uscita della BTS.

- Recupero Chiave dall'Authentication Center (AuC) :
    - Lo stesso attacco utilizzato per il recupero di *Ki* da una SIM card può essere utilizzata per recuperare la chiave *Ki* dall'AuC. Quest'ultimo deve rispondere alle richieste fatte dalla rete GSM e restituire triple valide da utilizzare nell' autenticazione della MS. La procedura di base è identica alla procedura utilizzata nella MS per accedere alla SIM. La differenza è che l'AuC è molto più veloce nel processare le richieste di quanto non lo sia la SIM card. La sicurezza dell'AuC gioca un ruolo fondamentale riguardo alla possibilità di eseguire l'attacco.

- Intercettazione delle chiamate:
    - Questa ultima tecnica è implementabile mediante diversi dispositivi come Monitor, cimici…
    - È comunque da precisare che : L'intercettazione e la codifica real-time di una chiamata via etere non è ancora praticabile.

11.8 Clonazione dei GSM

Dato che l'informazione riservata che rende possibile la clonazione dei cellulari GSM è memorizzata nelle schede smart card (carte SIM), è possibile catturare e decifrare questo codice riservato da qualsiasi tipo di scheda. In pratica è stata scoperta una falla nell'algoritmo COMP128 utilizzato in tutte le smart card SIM per la memorizzazione del codice identificativo personale.

11.A Bibliografia

- Apogeo - Segreti, Spie, Codi(ci)frati – C.Giustozzi – 1999
- Dispense Corso di "Sistemi di telecomunicazioni" Prof. Neri - Univ. Roma 3

12 La Pirateria Satellitare

Negli ultimi 20 anni si è andata sempre più diffondendo la pirateria satellitare che permette ad alcune persone, con modeste capacità tecniche, di creare delle wafer card (schede pirata) da inserire nel decoder per vedere abusivamente programmi trasmessi via satellite a pagamento. Per poter fare questo gli "hacker" devono poter acquisire le informazioni tecniche necessarie ad ottenere i codici di decriptazione del segnale protetto che poi mettono a disposizione di tutti attraverso internet.
Da vari siti vi è la possibilità di scaricare diversi software che permettono di programmare e quindi "innestare" questi codici nella memoria delle schede (smart card).

Alcuni compongono schede pirata al solo scopo di farne un uso personale, altri invece a scopo di lucro. Pertanto si può parlare di diversi comportamenti criminosi, distinti l'uno dall'altro:

- chi crea i programmi per fare wafer card o alterare le carte originali (smart card) per puro divertimento o per testare la propria abilità (hacker satellitari);
- chi programma le wafer card o manipola quelle originali in ambiente domestico per il solo scopo personale di vedere in frode i programmi televisivi a pagamento;
- chi sfrutta la propria capacità tecnica al fine di realizzare forti guadagni illeciti vendendo all'utente le wafer card (lamers in temine tecnico).

In alcuni casi queste tre attività possono essere riconducibili tutte ad una stessa persona. Sebbene comprare e assemblare i vari pezzi non sia un atto illecito il fenomeno si trasforma in un reato nel momento in cui la carta pirata è in condizione di accedere ai servizi a pagamento violando la legge sul diritto d'autore n. 633/1941 modificata dalla n. 248/2000. Rientra tra le violazioni, chiaramente, anche l'uso della carta originale (smart card) fatto in modo difforme dall'accordo di contratto.

I dati	Anno 2000	Primo trimestre 2001
Operazioni svolte	22	30
Persone arrestate	0	0
Persone denunciate	67	137
Materiale sequestrato		
Smart card	228	113
Wafer card	53	54
Decoder	127	124
Personal Computer	3	10
Kit per duplicazioni	14	17
Altro		14

Negli ultimi anni la Polizia Postale e delle Comunicazioni si è dedicata con particolare costanza e impegno al contrasto della pirateria satellitare esercitando controlli sulla regolarità degli abbonamenti e sulle specifiche tecniche dei prodotti utilizzati per la ricezione dei segnali tv. Ha esercitato un controllo continuo sulla rete internet e

mantenuto i rapporti con i gestori sulle nuove tecnologie e sullo studio delle contromisure elettroniche.

Effettua, inoltre, un costante monitoraggio ed analisi di tutti i siti che contengono notizie di carattere illecito, nonché dei forum e delle Chat, attivando accertamenti idonei all'identificazione di eventuali responsabili di attività illecite.

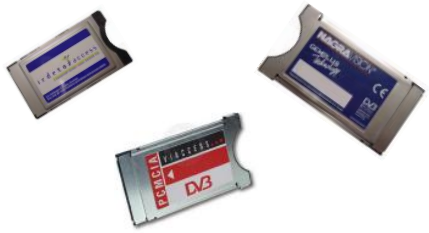
12.1 La trasmissione Satellitare

Il segnale criptato viene trasmesso dai gestori, sotto forma di onde radio, al satellite che le ritrasmette alle parabole sul territorio. L'abbonato riceve il segnale attraverso la parabola che a sua volta lo invia al ricevitore satellitare (decoder). Quest'ultimo, interfacciato ad una smart card fornita dal gestore e contraddistinta da un numero seriale associato all'abbonato, permette la visione in chiaro.

12.1.1 Sistemi di Codifica

La Pay TV e la Pay per View è basata su un segnale televisivo criptato attraverso metodi sempre più sofisticati quali:

- Irdeto;
- Nagra;
- Seca;
- Viaccess;
- NDS.



12.1.2 Ricezione e Decodifica

Attualmente per la ricezione di un segnale digitale codificato, si utilizzano ricevitori IRD (Integrated Receiver Decoder - ricevitore con decoder integrato).
L'integrazione dei circuiti di decodifica all'interno dei ricevitori può essere di due tipi:

- attraverso un sistema "on board" di tipo chiuso (i circuiti vengono assemblati sulla piastra madre dell'apparecchio)
- attraverso uno standard modulare aperto (come la Common Interface), basato su uno slot nel quale inserire il modulo di decodifica detto CAM (Conditional Access Module, ovvero Modulo d'Accesso Condizionato).

12.1.3 CAM

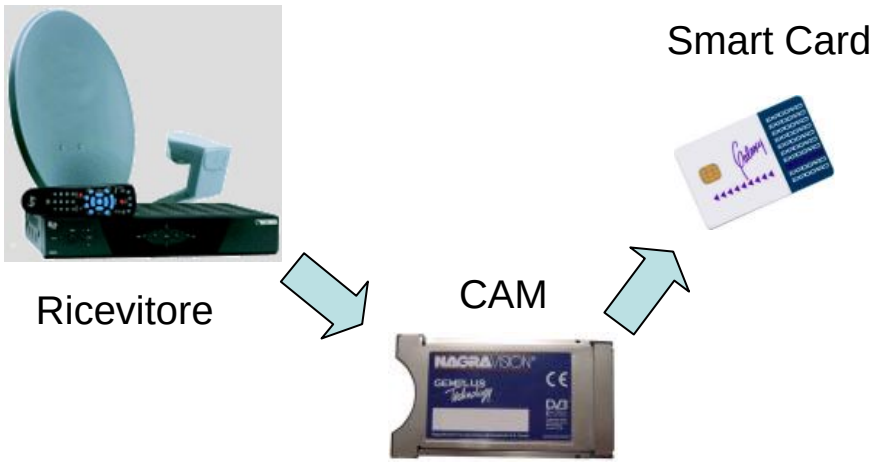
La CAM è un dispositivo preposto alla decodifica del segnale secondo il particolare sistema utilizzato. La decodifica è condizionata attraverso un continuo colloquio con la smart card per verificare che l'utente possieda il diritto alla visione.
I ricevitori COMMON INTERFACE dispongono di uno o più slot in cui inserire le CAM.

12.1.4 Smart Card

Supporto magnetico dove vengono conservati i dati che identificano un abbonato. Vengono consegnate dai gestori al momento della sottoscrizione del contratto. Possono essere divise in tre grandi categorie:

- solo memoria (documenti d'identità);
- memoria con logica di sicurezza (badge);
- memoria con CPU (sim-card).

12.1.5 Schema completo



12.2 Tecniche di Attacco

- La sicurezza delle smart card ha dei limiti già a livello fisico.
- Con appositi strumenti è possibile modificare strutturalmente la card in modo da leggere/scrivere e interpretarne il contenuto informativo.
- Durante una conferenza dell'Eurocrypt si è dimostrato che si può cortocircuitare una smart card in modo da poterla collegare tramite comunicazione seriale e conseguentemente decifrare ogni valore memorizzato.

Esistono due tipi di categorie di attacchi alle smart card:

- Tecniche di ingegneria inversa: si cerca di capire il funzionamento della smart card mediante la ricostruzione della logica interna del chip.
- Tecniche che si basano sul contenuto della EEPROM: si interfaccia la card con un pc per leggere e successivamente decifrare il contenuto della EEPROM.

12.2.1 Analisi dell'assorbimento elettrico

Questo tipo di attacco tende a mettere in relazione le variazioni di assorbimento elettrico, dovute alla commutazione dei "transistor", con i processi svolti dal microprocessore.

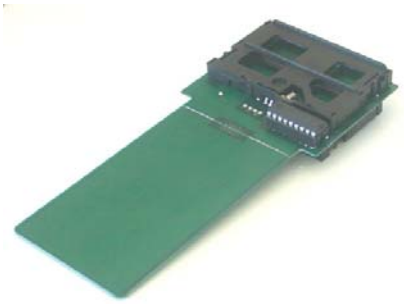
Una contromisura efficace adottata dai costruttori di Smart Card consiste nel disaccoppiare il "clock" fornito all'interfaccia dal "clock" del microprocessore e variarne in modo casuale la frequenza durante processi di calcolo interno.

12.3 Strumenti per l'Hacker

In questa sezione vengono passati brevemente in rassegna gli strumenti più utilizzati dai Pirati Satellitari per "aprire" i vari sistemi di criptaggio.

12.3.1 Dual Card o Blocker

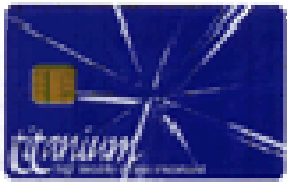
Interfaccia usata tra smart card e decoder. E' costituita da un microchip posto sulla sua superficie che analizza i segnali scambiati tra la CAM e la Smart Card. Lo scopo e quello di filtrare tutti i segnali destinati alla disabilitazione dei canali ed impedendo la riprogrammazione della card.



12.3.2 Titanium Card

Smart Card in grado di sostituire (correttamente programmata) qualsiasi carta in circolazione ad oggi. Le caratteristiche rilevanti sono:

- Type: Smartcard
- Flash: 32 kB (28 kB free)
- RAM: 1024 Byte
- EEPROM: 32 kB
- Crypto: Yes (RSA)
- Protokoll: T0, T1, TE
- Language: ASM, (C)
- Programmable @ 3.57 MHZ



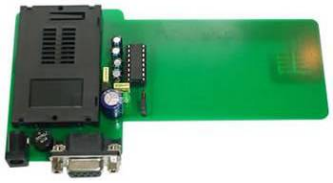
12.3.3 Smart Mouse

E' il più diffuso programmatore di smart card, da collegare ad un computer attraverso cavo seriale. Utilizzando appositi programmi unitamente a file ".BIN" opportuni, consente di "resuscitare" card con abbonamenti scaduti e di programmare le Wafer Card.

12.3.4 Season

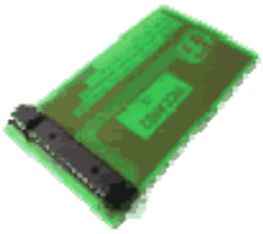
Interfaccia utilizzata per monitorare il dialogo tra il sistema d'accesso condizionato (CAM) e la smart card, al fine di individuare:

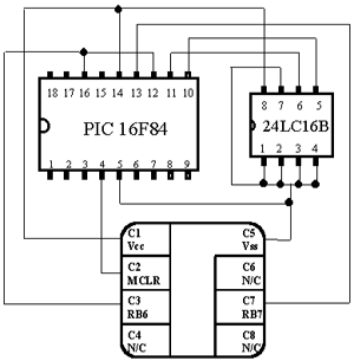
- i comandi di abilitazione e disabilitazione;
- le chiavi per la programmazione.



12.3.5 Wafer Card

E' un circuito elettronico che deve essere inserito nel decoder. E' costituito da una scheda rigida, da una memoria (EEPROM) dove sono contenute le informazioni per far funzionare il circuito e un microprocessore (PIC) che consente di elaborare le informazioni contenute nella EEPROM per mettere in chiaro il segnale criptato.





12.4 Dall'HW all'emulazione SW

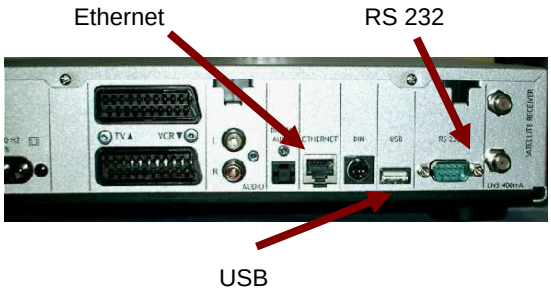
Gli strumenti appena illustrati sono dispositivi HW che contenevano del SW in grado di "agirare" le protezioni introdotte dalle varie codifiche proprietarie. L'incremento delle prestazioni dei calcolatori (v. Legge di MOORE) ha fatto si che la tendenza attuale per "craccare" i sistemi di codifica si sia spostata verso l'emulazione SW piuttosto che costruire materialmente apparati del genere. In questo modo non è più necessario apportare delle modifiche circuitali sulle Wafer Card oppure riprogrammare continuamente le Smart Card. Tutto questo porta innumerevoli vantaggi, come la possibilità di installare diversi S.O. dedicati nei decoder emulati che gli stessi gestori forniscono. Purtroppo in questo modo, l'interscambio tra Pirati Satellitari è facilitato (es. comunità on-line segrete su Web).

12.4.1 Caso di Studio (NDS – Sky Italia)

L'ultimo crack ha sfruttato il tele aggiornamento dei gold box funzionanti con il sistema SECA al nuovo NDS. SKY Italia, proprietaria di NDS, per ovvi motivi, non ha voluto rilasciare le specifiche per non favorire i malintenzionati. In questo modo, per non sostituire tutti i decoder in circolazione, si è reso necessario aggiornare il software dei vari ricevitori. A questo punto gli Hacker hanno sviluppato un SW che emulava alla perfezione un vecchio gold box con il quale è stato possibile scaricare l'aggiornamento e manipolarlo. Così è stato reso possibile la visione di programmi satellitari a pagamento anche con il gestore della TV satellitare in Italia. Rimane un sistema non alla portata di tutti, poiché necessita di continui aggiornamenti e capacità tecniche innumerevoli. Tutto questo è stato favorito da calcolatori in grado di emulare qualsiasi decoder e con gli strumenti giusti (programmi scaricabili dalla rete) anche qualsiasi CAM in circolazione. Un esempio è il DREAMBOX. L'aspetto è quello di un normale decoder, ma all'interno si scopre un calcolatore a tutti gli effetti Linux-based.

12.4.2 Il DREAMBOX

Questo dispositivo (calcolatore) è in grado di ricevere e codificare, per mezzo dell'emulazione di tutte le CAM e dei vari S.O. dei decoder, qualsiasi programma trasmesso dai satelliti puntati dalle parabole. Vi è la possibilità di registrare *on-the-fly* qualsiasi programma televisivo ricevuto sul proprio Hard-Disk. Inoltre consente interazioni con l'utente in maniera user-friendly.



12.A Conclusioni

Il contenuto di queste slide si trova liberamente sul Web perchè non bloccato da organi di vigilanza o di polizia giudiziaria. Il mio compito e' stato quello di descrivere ad alto livello la pirateria satellitare creando questa presentazione con lo scopo di illustrare le tecnologie e le metodologie usate in questo settore.

12.B Bibliografia

- http://www.poliziadistato.it
- http://www.tv-satellitare.com
- http://www.irdeto.com
- http://www.nagra.com
- http://www.viaccess.com
- http://www.nds.com
- http://www.4freeboard.to/board/index.php
- http://csa.irde.to/index.html
- http://www.eurosatellite.chaosmagic.com
- http://www.cryogenteam.it
- http://www.duwgati.com/de/home.php