CRITTOGRAFIA NELL'AMBITO DELLE SMART CARD

Sicurezza, tecniche di attacco e qualche scenario specifico

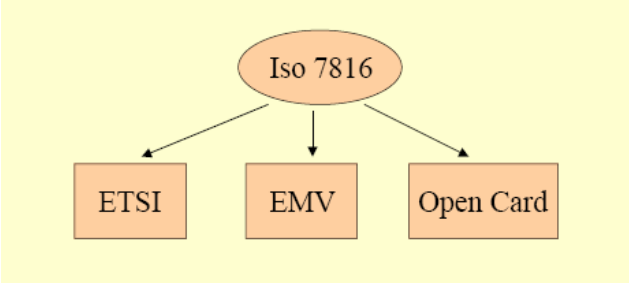
Parisi Francesca

Naclerio Fabio

Paternesi Noemi

Di Maria Valerio

STANDARD

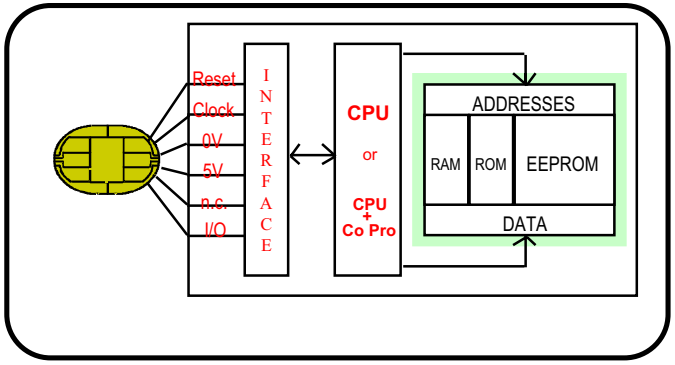


Voluti per garantire una lunga durata del sistema ed un'interoperabilità di componenti di differenti costruttori.

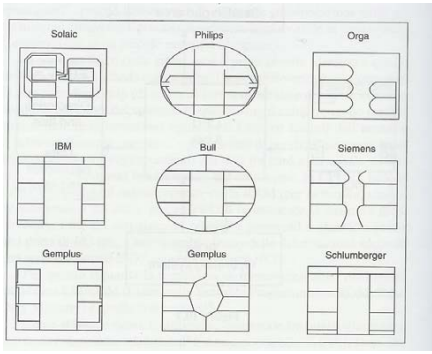
COSA SONO LE SMART CARD

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)



TIPI DI SMART CARD



Smart card a contatto

- ✓Composte da placche utilizzate per fornire la necessaria energia e per comunicare attraverso contatti elettrici diretti con il lettore.
- ✓I lettori per le smart card a contatto sono di solito dispositivi separati da collegare alla porta seriale od USB.

TIPI DI SMART CARD

Smart card senza contatto

✓Non hanno connettori sulla propria superficie.

✓ La connessione tra il lettore e la scheda viene effettuata via radiofrequenza (RF).

✓Le schede contengono una piccola spira di filo conduttore utilizzata come induttore per fornire energia alla scheda e per comunicare col lettore.

✓I lettori di smart card di solito si collegano al computer per mezzo della porta seriale od USB.

✓I lettori per smart card senza contatto possono avere o meno un'alloggiamento.

SMART CARD A MEMORIA

✓Sono le smart card più diffuse e meno costose.
✓Contengono una memoria permanente EEPROM (Electrically Erasable Programmable Read-Only Memory).
✓Quando si rimuove la scheda dal lettore e l'energia viene interrotta la scheda salva i dati.
✓I dati possono essere bloccati con un PIN (Personal Identification Number), la propria parola chiave.
✓I PIN sono composti da 3 ad 8 numeri che vengono scritti in un file speciale presente nella scheda.
✓Questo tipo di scheda non consente la crittografia
✓Vengono utilizzate per contenere credito telefonico, biglietti per il trasporto o denaro elettronico.

TIPI DI SMART CARD

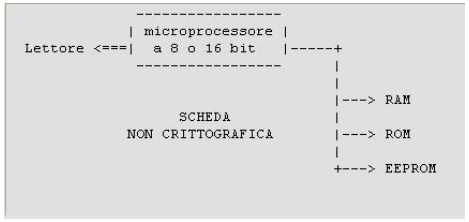
Schede combinate

✓Ha un blocco di contatti per la transazione di dati voluminosi 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.

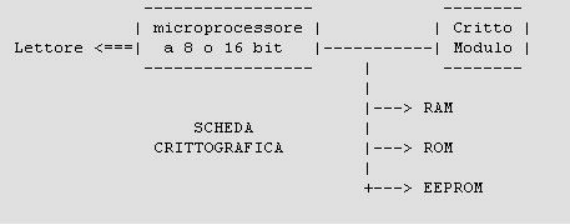
SMART CARD A MICROPROCESSORE

✓Hanno RAM, ROM e EEPROM con un microprocessore a 8 o 16 bit.
✓Nella ROM c'è un sistema operativo per gestire il file system presente nella EEPROM e per eseguire le desiderate funzioni nella RAM.
✓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.



SMART CARD A MICROPROCESSORE

✓Si ha l'aggiunta di un crittomodulo.
✓Si ha la necessità di aggiungere un componente per accelerare le funzioni crittografiche (frequenza interna dei microcontrolli compresa tra 3 e 5 MHz).
✓Sono più costose di quelle non crittografiche.



IL SISTEMA OPERATIVO DELLE SMART CARD

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**)**

✓ JavaCardOS

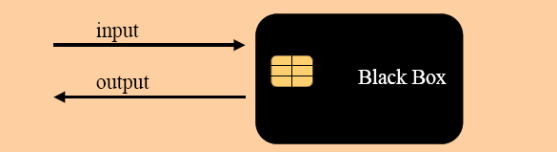
✓MULTOS

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



LE CARTE INTELLIGENTI

Per via della presenza della CPU, le smart card sono anche dette *carte intelligenti* poiché consentono di effettuare manipolazioni sulle informazioni attraverso l’utilizzo di software aggiornabile in tempo reale.

L’intelligenza delle smart card consente:

✓Implementazione della maggior parte delle tecniche crittografiche moderne

✓Rende molto più sicura una smart card rispetto ad una comune carta magnetica.

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

INTEGRITA' DEI DATI

Per integrità dei dati si intende la corretta trasmissione dei dati tra sorgente e destinatario senza alcun tipo di alterazione dell'informazione.

✓Viene garantita da sofisticate tecniche crittografiche dette *check digits*.

✓ Si usano delle procedure dette *hashing* che numericamente vincolano ad un insieme stabilito di valori numerici, un altro insieme di valori calcolati sulla base dei primi.

INTEGRITA' DEI DATI

Algoritmi Hash

I principali algoritmi hash utilizzati per garantire l'integrità dei dati nelle smart card sono:

✓SHA-1 (Secure Hash Algorithm) che produce un hash di 160 bit per un insieme informativo di valori numerici di 2^{64} bit di lunghezza al massimo.

✓MD5 (Message Digest 5) che produce un hash di soli 128 bit per un totale di 16 caratteri.

INTEGRITA' DEI DATI: SHA-1

Un gruppo di ricerca dell'Università di Shandong ha pubblicato un articolo che descrive alcune tecniche di attacco che riducono notevolmente, di quasi 2.000 volte, il tempo necessario a compromettere SHA-1.

Anche se la tecnica sarebbe molto difficile da usare in pratica, di fatto compromette l'integrità dell'algoritmo e potrebbe portare a metodi più avanzati e più pratici. Cioè SHA-1 potrebbe diventare inutile. L'effetto sarebbe molto grave: coinvolgerebbe, in una specie di reazione a catena, una lunghissima lista di prodotti di sicurezza per Internet che sfruttano SHA-1 per generare firme digitali. La maggior parte dei protocolli Internet, primo fra tutti SSL, usano SHA-1.

L'articolo dei tre ricercatori cinesi, Xiaoyun Wang, Yiqin Lisa Yin e Hongbo Yu, si chiama "Collision search attacks on SHA-1" e descrive come utilizzare il "metodo delle collisioni" per rompere molto più rapidamente l'algoritmo.

Una "collisione" è un evento in cui due messaggi hanno il medesimo valore di 'hash'. Questo fenomeno rende, in teoria, possibile generare artificiosamente firme valide sfruttando SHA-1. Nella crittografia ci si affida al criterio della "non repudiation" degli algoritmi, vale a dire che si prende per buono il concetto per cui due 'hash' identici non possono essere stati creati da due soggetti diversi.

Anche se la ricerca degli scenziati cinesi accorcia notevolmente i tempi, rompere SHA-1 non è esattamente alla portata di tutti. Un normale pc ci impiegherebbe circa 1.000 anni. Ma, potrebbe essere un metodo pratico per alcune entità governative (per esempio NSA) e qualche corportation molto, molto facoltosa.

Purtroppo una volta che un algoritmo è stato rotto, diventa relativamente semplice per altri ricercatori raffinare il processo e ottenere risultati migliori. L'articolo non è ancora stato pubblicato, ma potrebbe apparire presto sul sito della International Association for Cryptographic Research.

Anche se gli attacchi pratici sembrano lontani, i crittografi dovranno decidere presto se rimpiazzare SHA-1 entro i prossimi due anni. Allo stesso modo le aziende che si affidano a SHA-1 per i protocolli di comunicazione sicura dovranno decidere il da farsi.

AUTENTICAZIONE

Consente di stabilire se un insieme informativo proviene realmente dalla fonte originaria.

✓Si aggiunge una scansione particolare del contenuto informativo dell'insieme di dati all'insieme informativo da trasmettere per scongiurare eventuali manomissioni.

✓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.

AUTENTICAZIONE

Algoritmi 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:

✓DSA (Digital Signature Algorithm) utilizza una chiave privata di lunghezza variabile tra 512 e 1024 bit

✓RSA utilizza chiavi private lunghe fino a 2048 bit

IRRIPRODUCIBILITA'

Bisogna garantire che la scansione del contenuto informativo dell'insieme di dati non possa essere copiata.

✓Chiunque con un minimo di attrezzatura può copiare il contenuto informativo di un dispositivo digitale e la copia risultante sarà indistinguibile dall'originale.

RISERVATEZZA

Bisogna evitare che un intruso possa catturare e decifrare le operazioni interpretando, di conseguenza, il contenuto informativo della smart card.

✓Su una smart card si può implementare qualsiasi tipo di algoritmo crittografico.

SICUREZZA FISICA DELLE SMART CARD

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**

SICUREZZA LOGICA DELLE SMART CARD

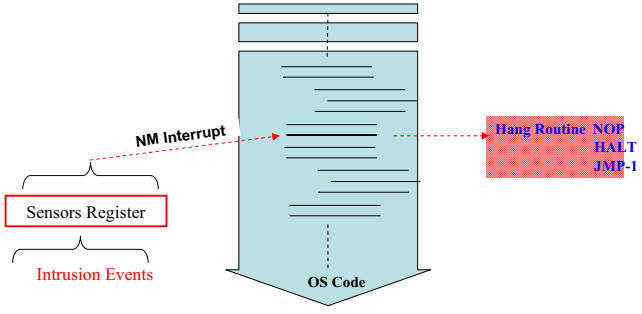
La sicurezza logica controlla l'accesso alle informazioni contenute nella smart card tramite:

- ✓ 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).

CONTROMISURE PRINCIPALI

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



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)

LE 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.

CRYPTOKI

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.

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.

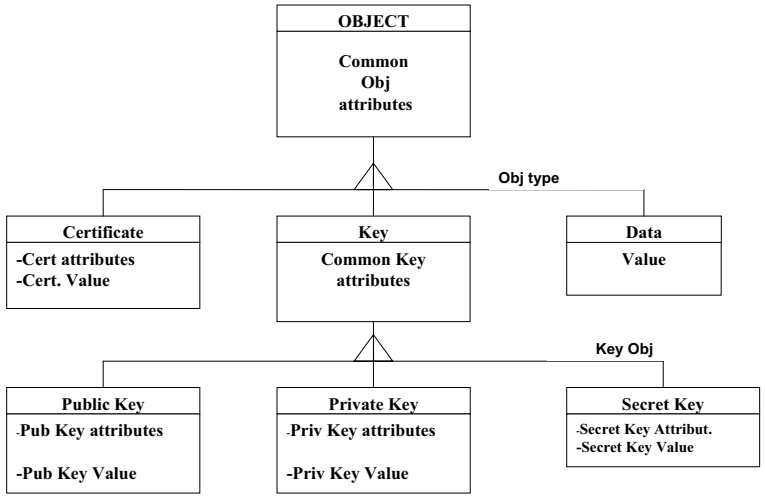
✓Vincolano all'utilizzo del dispositivo crittografico per cui sono state sviluppate ovvero non consentono a Smart Card di differenti fornitori di poter operare sulla stessa piattaforma applicativa.

CRYPTOKI

Il "Token"

- ✓ 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

RAPPRESENTAZIONE A OGGETTI DEL TOKEN



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.

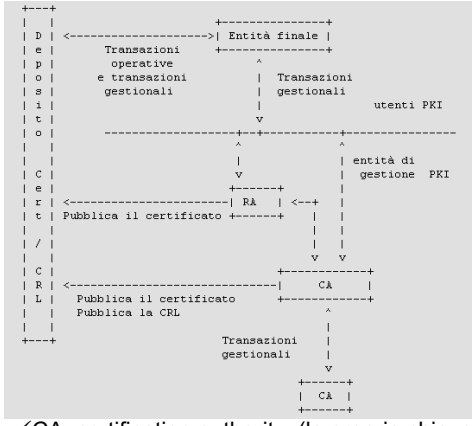
✓ Quando il colloquio è in modalità "web browsing" viene utilizzato il protocollo TLS/SSL (Transport Layer Security/Secure Socket Layer)

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

LE FUNZIONI **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

RAPPORTO TRA SMART CARD E PKI

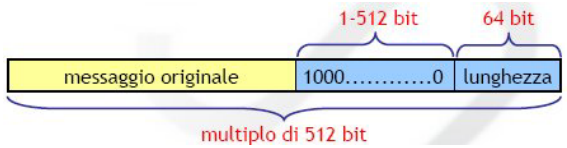


✓entità finale: utente dei certificati PKI e/o il sistema utente finale che è il soggetto del certificato;
✓RA: registration authority, ovvero un sistema opzionale cui una CA delega certe funzioni gestionali; (in alcune implementazioni, dove tu registri te stesso nel sistema)

✓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.

- ✓MD5
- ✓DSA
- ✓RSA(cenni)
- ✓Carta Di Identità Elettronica (CIE)

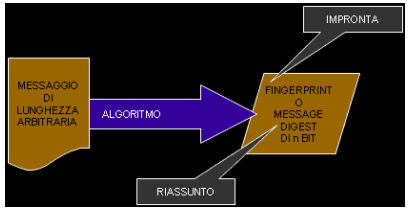
Naclerio Fabio



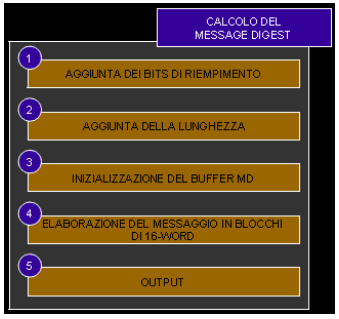
Aggiunta bits di riempimento: il messaggio viene sempre esteso (padding) così che la sua lunghezza in bits sia congruente a 448 mod 512. Il primo bit di estensione è sempre un '1' seguito da una serie di '0' mentre il numero di bits di estensione va da un minimo di 1 ad un massimo di 512.

Aggiunta della lunghezza: viene aggiunta una rappresentazione a 64-bit della lunghezza del messaggio (b) prima del riempimento (modulo 64)

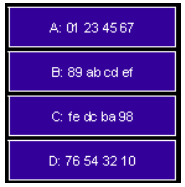
L'algoritmo MD5 genera un'impronta, chiamata anche fingerprint o message digest, della lunghezza di 128 bits, di un messaggio di lunghezza arbitraria.

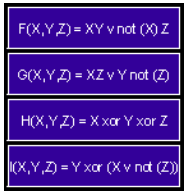


L'algoritmo è suddiviso in cinque fasi principali:

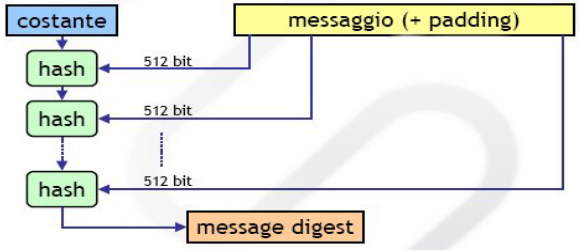


Inizializzazione del buffer MD (initial variable/chaining variable): si tratta di un buffer di quattro word (A, B, C, D) a 32-bit aventi questi valori esadecimali di inizializzazione (la prima word per prima):





Elaborazione del messaggio (compression function): vengono definite quattro funzioni ausiliare che ricevono in ingresso un blocco di 32-bit e il digest fino a questo momento prodotto e producono in uscita un solo blocco di 32-bit che rappresenta il nuovo digest.



DSA

- ✓ Creato da Schnorr e ElGamal nel 1994
- ✓ Si basa sul problema dei logaritmi discreti
- ✓ Riferito anche come DSS (Digital Signature Standard) del NIST (FIPS 186)
- ✓ Nato appositamente come algoritmo per la generazione di firme digitali ed utilizza chiavi con lunghezza da 512 a 1024 bit

Generazione delle chiavi:

1. Scegliere un numero primo p con $512 \leq p \leq 1024$ e $p \bmod 64 = 0$
2. Scegliere un numero primo q di 160 bit, tale che $p - 1 = qz$ con z appartenente ad N
3. Scegliere h *appartenente ad* N con $1<h<p-1$ tale che $g=hz \bmod p < 1$
4. Scegliere x a caso, con $0 < x < q$
5. Calcolare $y = g^x \bmod p$

RSA

L'analisi dell'algoritmo viene suddivisa in due parti:

- ✓ generazione della coppia di chiavi
  - vengono scelti due numeri primi **p**, **q** molto grandi
  - viene calcolato **n=pq**, e la funzione di Eulero **Φ(n) = (p - 1)(q - 1)** dopo di che i due primi **p**, **q** vengono eliminati
  - si sceglie un intero **e** minore di **Φ(n)** e primo con esso
  - utilizzando la versione estesa dell'algoritmo di Euclide viene calcolato l'intero **d** così da avere **e * d = 1 mod Φ(n)**
  - vengono resi pubblici i valori **e**,**n** che costituiscono la chiave pubblica e mantenuto segreto **d** che, utilizzato con **n** rappresenta la chiave privata.
- ✓ utilizzo delle chiavi
  - cifratura
  - decifratura
  - firma
  - verifica

DSA

- ✓ La chiave pubblica è rappresentata da (p, q, g, y) e quella privata da x.

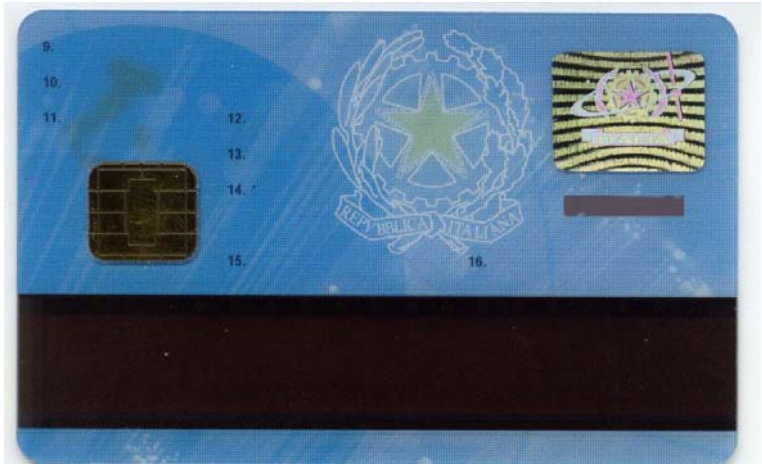
Firma di un messaggio:

1. Scegliere un valore a caso s (detto *nonce*), con $1 < s < q$
2. Calcolare $s1 = (g^s \bmod p) \bmod q$
3. Calcolare $s2 = (H(m) - s1x)s\text{-}1 \bmod q$, dove $H(m)$ è la funzione hash SHA-1 applicata al messaggio m

La firma è rappresentata da ($s1$, $s2$).

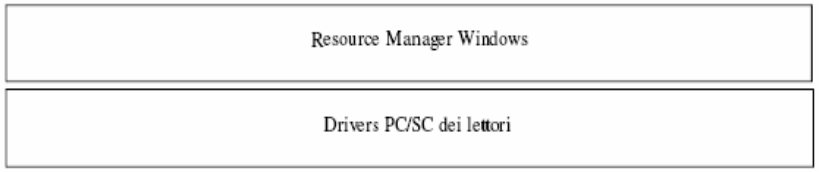
CARTA D'IDENTITA' ELETTRONICA

CARTA D'IDENTITA' ELETTRONICA



L'ARCHITETTURA

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.

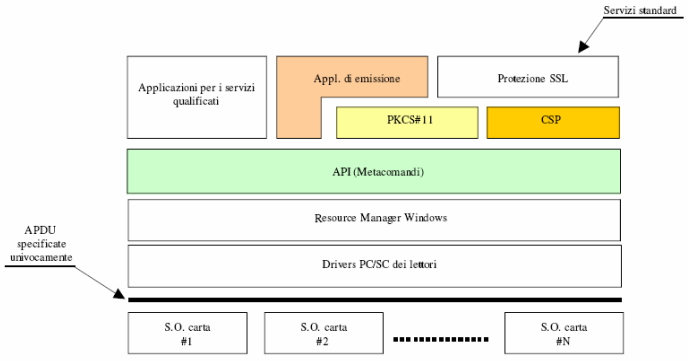


Lo strato intermedio PKCS#11 (o in ambiente Microsoft il CSP) può essere utilizzato dagli attuali browser per funzioni native di sicurezza che sfruttano il protocollo SSL V3

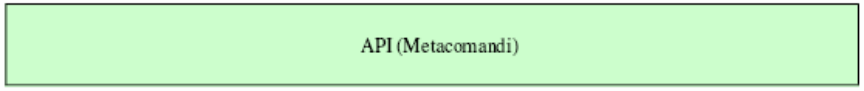
L'ARCHITETTURA

- ✓ 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.



L'ARCHITETTURA



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).

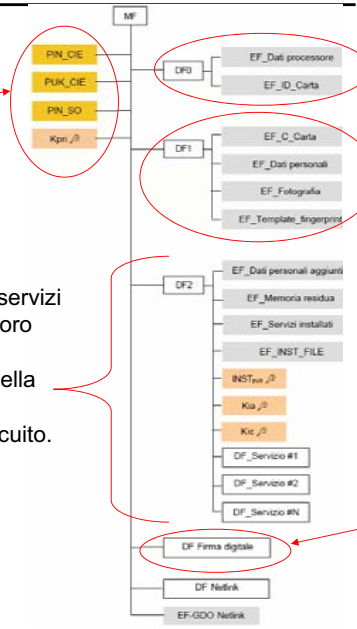
METACOMANDI CIE

```
#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
```

FILE SYSTEM nel MICROCIRCUITO

Qui vengono memorizzate tutte le informazioni di sicurezza



Qui vengono memorizzate le informazioni base della carta

Qui vengono memorizzate le Informazioni del titolare

Qui vengono installati i servizi che necessitano, per il loro funzionamento, di una struttura dati riservata nella memoria riscrivibile (EEPROM) del microcircuito.

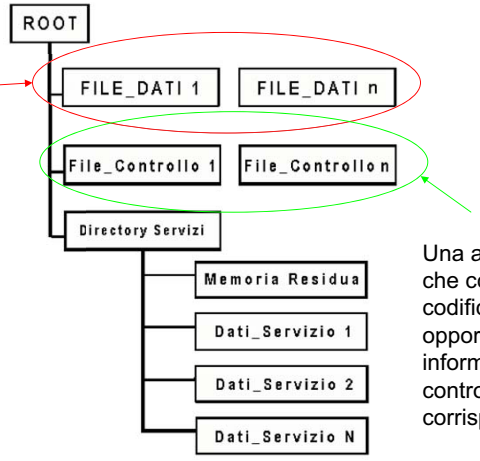
Qui viene memorizzata la firma digitale del titolare.

METACOMANDI CIE

- ✓ 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);*

STRUTTURA DELLE INFORMAZIONI SULLA BANDA OTTICA

Una area dati che contiene, codificati in record di formato opportuno (Rd), i necessari dati della carta



Una area di controllo che contiene, codificate in formato opportuno (Rc), le informazioni di controllo e verifica dei corrispondenti Rd.

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.

AFFIDABILITA' DEI DATI

- ✓ **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.

AFFIDABILITA' 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.

AFFIDABILITA' DEI DATI

- ✓ **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.

    - ✓ .....

AFFIDABILITA' DEI DATI

✓ **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.

ALGORITMI

✓ 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

SIM CARD & CRITTOGRAFIA

Paternesi Noemi

Introduzione

✓ Un altro settore in cui la crittografia trova parecchie applicazioni è la telefonia digitale.

✓ Le normali conversazioni telefoniche analogiche non vengono cifrate perché non è interesse dell'operatore (Esistono però strumenti – Scrambler - per la cifratura delle comunicazioni)

✓ Per quanto riguarda la telefonia digitale, le comunicazioni vengono criptate solamente per quanto riguarda la trasmissione via etere, la comunicazione a terra viaggia invece in chiaro.

Sicurezza nel GSM

- ✓ 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
- ✓ La chiamata viene digitalizzata, cifrata e inviata alla centrale ricevente più vicina che la decifra e la invia in chiaro al numero telefonico corrispondente.

La crittografia del GSM

- ✓ GSM si avvale di alcuni algoritmi crittografici di tipo simmetrico:
  - A3
  - A5
  - A8
- ✓ A3 e A8 sono utilizzati per la procedura di autenticazione
- ✓ A5 è usato per la trasmissione della comunicazione vocale

Informazioni base

- ✓ L'abbonato è identificato univocamente dal codice IMSI e da una chiave personale di autenticazione *Ki.* Questa chiave è contenuta nella SIM e in un database centrale (HLR) della rete di appartenenza.
- ✓ L'innovazione particolare è che queste informazioni non vengano trasmesse sul canale radio per di garantire maggiore sicurezza e protezione.

A3, A8, A5

- ✓ A5 è un algoritmo "stream chiper" (opera su singoli bit cifrandoli uno alla volta)
- ✓ A3 e A8 sono anche chiamati nel gergo delle funzioni hash "key-dependent" (dipendenti da una chiave) e "one-way" (cioè è particolarmente difficile calcolarne l'inversa).
- ✓ 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)).
  - In sostanza una funzione hash è una trasformazione che lega un numero, ad un insieme di valori numerici che rappresentano l'informazione da autenticare, nel nostro caso dati binari relativi alla comunicazione cellulare.

Sicurezza nel 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)

Fasi

✓Fase di autenticazione

✓Fase di comunicazione

Sicurezza nel GSM

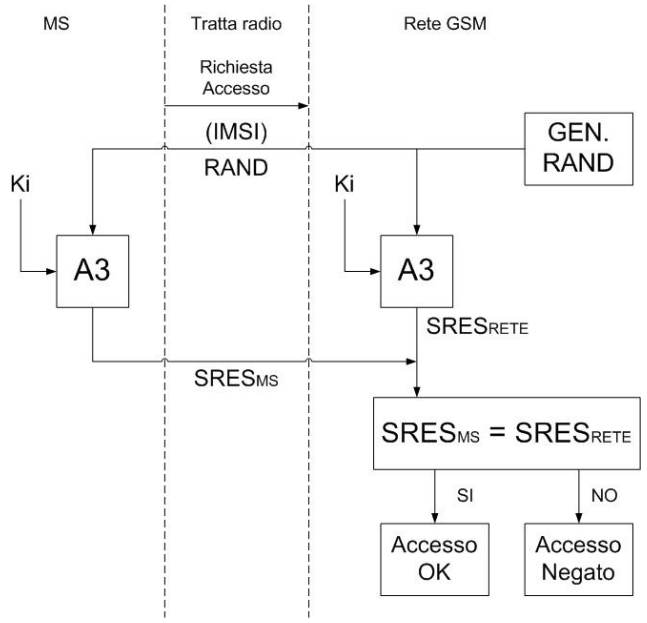
- ✓ Nella SIM sono memorizzate le seguenti informazioni:
  - il codice IMSI
  - la chiave personale di autenticazione Ki
  - l'algoritmo A8 che genera la chiave temporanea Kc
  - l'algoritmo A3 di autenticazione
  - il codice PIN personale
- ✓ Nell' ME è memorizzato l'algoritmo A5 di cifratura per i dati relativi alla comunicazione
- ✓ Nelle BTS sono memorizzati l'algoritmo A5 per la decifrazione dei messaggi e la chiave temporanea Kc. Inoltre la BTS ha accesso all'HLR

Autenticazione

- ✓ Tra SIM e centro di autenticazione AuC (Authentication Center) presente nella stazione BTS.
- ✓ Quando?
  - Ogni volta che utilizziamo il cellulare per ricevere o effettuare chiamate,
  - per aggiornare la posizione della stazione mobile
  - quando vengono eseguite le operazioni di attivazione, disattivazione, interrogazione dei servizi supplementari.

Autenticazione

- ✓ Avviene tramite una procedura detta challenge-response:
  - ad 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 riceve il RAND, lo utilizza come input per l'algoritmo A3 insieme alla chiave personale Ki, il risultato (SRES), di 32 bit, viene spedito (response) all' AuC per l'autenticazione.

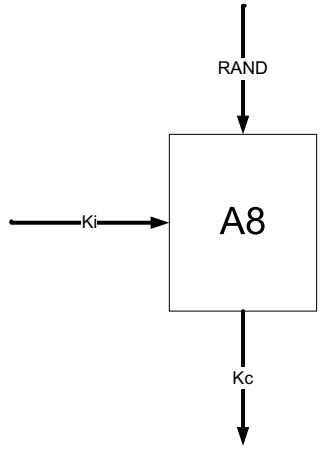


Autenticazione

- Anche l'AuC ha calcolato il SRES con lo stesso RAND e con la stessa chiave Ki, che conosce avendo identificato l'utente (la chiave è memorizzata nell'HLR dell'AuC)
- Quindi l'AuC confronta il suo SRES con l'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
- Se l'autenticazione va a buon fine, l'MS e la stazione base calcolano la chiave Kc, con l'algoritmo A8, il RAND e Ki, che servirà per codificare la comunicazione.

Autenticazione

- ✓ 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



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

Riservatezza delle comunicazioni

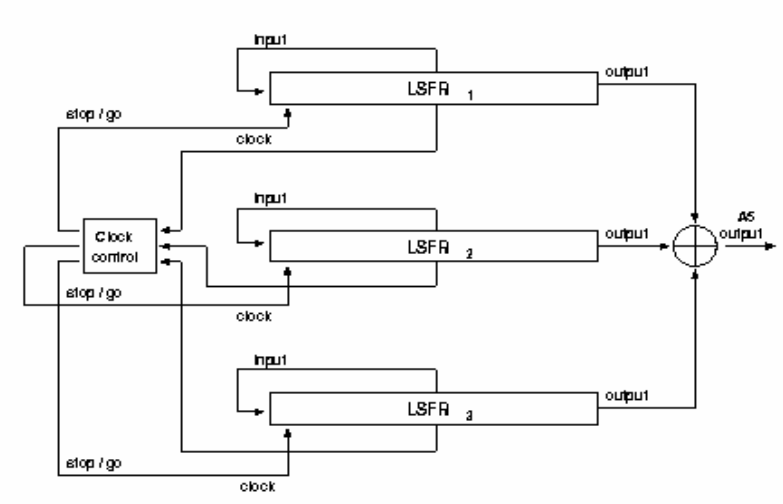
- ✓ Viene effettuata tramite l'algoritmo A5.
- ✓ A5 usa una chiave di cifratura Kc di 64 bit e il numero della trama TDMA di 22 bit per produrre una sequenza di 114 bit (keystream) che viene utilizzata per crittografare i 114 bit significativi di ogni burst attraverso uno XOR.
- ✓ L'algoritmo consiste in tre registri a scorrimento a retroazione lineare rispettivamente di 19, 22 e 23 bit, sincronizzati.
- ✓ La somma dei tre registri è 64 e infatti la chiave di cifratura di 64 bit è utilizzata per inizializzarli ad ogni sessione.

Comp128

- ✓ Il COMP128 e' considerato un algoritmo debole
- ✓ In generale anche gli altri algoritmi utilizzati dal GSM lo sono. Infatti:
  - gli ultimi 10 bit della chiave di sessione kc sono posti uguali a zero.

  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 .

A5 - Registri a scorrimento



A5 - Registri a scorrimento

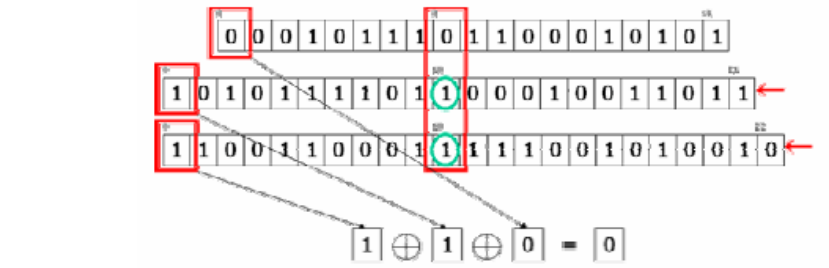
- ✓ Dopo il caricamento dei bit della chiave di sessione ciascuno dei 22 bit del numero di frame viene messo in XOR con i tre valori di feedback dei registri stessi.
- ✓ Durante il caricamento di ciascun bit del numero di frame, vengono shiftati i registri il cui bit centrale concorda con il bit di maggioranza.
- ✓ I 3 registri sono sincronizzati in base al bit centrale di ognuno

A5 - Registri a scorrimento

- ✓ 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.

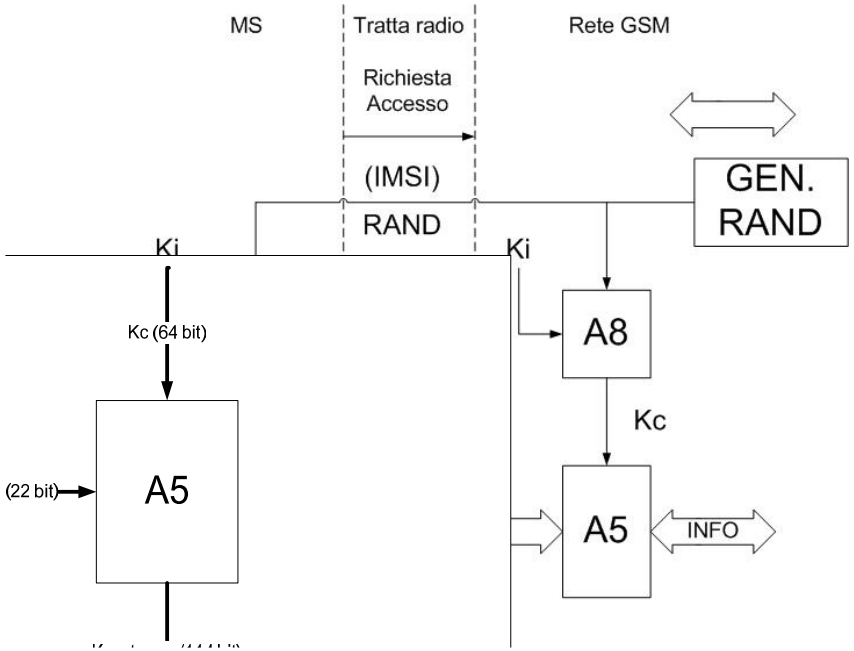
A5 - Registri a scorrimento

- ✓ 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.



A5

- ✓ È utilizzato per la cifratura/decifratura dei messaggi tramite l'utilizzo della chiave Kc generata dall'algoritmo A8 mediante l'utilizzo del numero casuale RAND e della chiave personale Ki.
- ✓ 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.
- ✓ 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.



Attacchi alle SIM Card

✓ SIM Card (Recupero della chiave Ki)

– Attacchi Logici :
  - via etere, Un attaccante potrebbe impersonare la BTS legittima inviando alla MS obiettivo delle challenge per risalire alla chiave segreta mediante le risposte a queste challenge.

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

Attacchi alle SIM Card

✓ Algoritmi di Cifratura (Attacchi all'Algoritmo A5)

– Attacco Brute-Force :
  - Real-time non è realizzabile.
  - 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) :
  - Riduce la complessità da 2^{54} tentativi dell'attacco di forza bruta a 2^{45}.
  - Tenta di determinare lo stato iniziale degli **LFSR** da una sequenza di **keystream** conosciuta.
  - E' sufficiente conoscere solo **64 bit consecutivi** della keystream calcolati dalle coppie testo in chiaro-testo cifrato note.

Attacchi alle SIM Card

– Rottura dell'Algoritmo COMP128
  - Attacco Chosen-Challenge:
    – 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.

Attacchi alle SIM Card

- ✓ Architettura di Rete (Insicurezza strutturale della Rete)
  - Intercettazione:
    - L'intercettazione e la codifica real-time di una chiamata via etere non è ancora praticabile
  - 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.

La Pirateria Satellitare

uso illecito delle Smart Card e simili

Valerio Di Maria

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.

Introduzione

- ✓ 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.

Introduzione

- ✓ 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).

Introduzione

- ✓ 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.

Introduzione

- ✓ 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.

Alcuni Dati…

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

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.

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).

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.

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

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).

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.

Schema completo

Ricevitore

CAM

Smart Card

Tecniche di Attacco

- ✓ 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.

Strumenti per l'Hacker

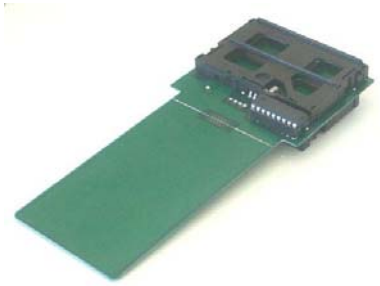
- ✓Dual Card o Blocker
- ✓Titanium Card
- ✓Smart Mouse
- ✓Season
- ✓Wafer Card
- ✓Emulatori

Titanium Card

- ✓ 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

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.

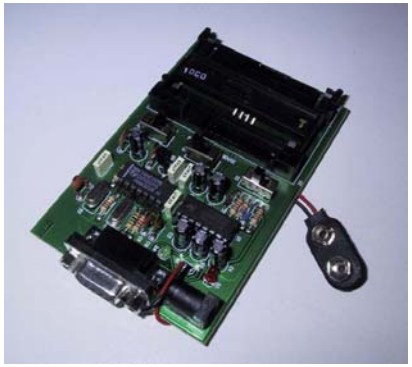


Season

- ✓ 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.

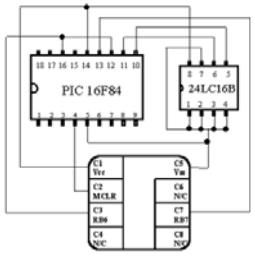
Smart Mouse

- ✓ 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.



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.



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 assemblare materialmente dispositivi del genere.

Dall'HW all'emulazione SW

- ✓ In questo modo non è più necessario apportare delle modifiche circuitali sulle Wafer Card oppure riprogrammare le Smart Card.
- ✓ Vi è la possibilità di installare diversi S.O. dedicati nei decoder emulati che gli stessi gestori forniscono.
- ✓ L'interscambio tra Pirati Satellitari è facilitato (es. comunità on-line segrete).

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 del sistema 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.

Caso di Studio (NDS – Sky Italia)

- ✓ 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 es. è il DREAMBOX. L'aspetto è quello di un normale decoder, ma all'interno si scopre un calcolatore a tutti gli effetti Linux-based.

Caso di Studio (NDS – Sky Italia)

- ✓ Dove hanno agito i Pirati?
  - – Hanno sviluppato un SW che emulava alla perfezione un vecchio gold box con il quale è stato possibile scaricare l'aggiornamento e manipolarlo.
- ✓ In questo modo è stata resa 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 è necessita capacità tecniche elevate.

Il Dreambox

- ✓ E' in grado di ricevere e codificare, per mezzo dell'emulazione di tutte le CAM e dei vari S.O. dei decoder, qualsiasi programma TV trasmesso dai satelliti puntati dalle parabole.
- ✓ E' in grado di registrare con qualità digitale (MPEG-2) qualsiasi evento sul proprio HD.
- ✓ Consente interazioni con l'utente in maniera user-friendly.

Il Dreambox

Processore IBM

Hard-Disk

Connettori Scart

Il Dreambox

Ethernet

RS 232

USB

Fine

Grazie per l'attenzione…