# 7 Sicurezza

In tutti i sistemi di telecomunicazione mobile, quindi anche nel GPRS, il problema della sicurezza è tra i più rilevanti. Infatti, l'interfaccia radio si presta maggiormente a intercettazioni e intromissioni indebite rispetto ad una rete cablata. Le caratteristiche di mobilità proprie del GSM/GPRS impediscono inoltre di conoscere a priori l'effettiva identità di chi effettua un tentativo di accesso alla rete. D'altra parte, la necessità di comunicare via radio l'identità dell'utente introduce un problema di privacy.

Le caratteristiche di sicurezza incluse nello standard GPRS hanno lo scopo di evitare l'uso non autorizzato del servizio e di assicurare la riservatezza dei dati trasmessi e delle informazioni sull'identità dell'utente. Così come nel GSM, le due chiavi utilizzate sono dette *Individual subscriber authentication key* (Ki) e *Cipher key* (Kc). La chiave Ki è assegnata dal gestore all'utente al momento della registrazione, assieme all'IMSI, ed è memorizzata nella carta SIM dell'utente e nell'AuC del gestore. La chiave Kc è invece generata ogni volta che l'utente effettua l'autenticazione, sulla base della Ki e di un numero casuale. Nel GPRS è stato definito un particolare algoritmo di cifratura (A5), ottimizzato per la gestione di pacchetti di dati, che si aggiunge agli algoritmi propri del GSM.

## 7.1 Autenticazione dell'utente

In vari sistemi, l'autenticazione consiste nell'uso di un codice PIN segreto come mezzo per identificare l'utente. Tale metodo non è molto sicuro, poiché in sistemi di comunicazione senza filo è facile intercettare il codice durante la trasmissione e violare la riservatezza dei dati. Il codice PIN, infatti, viene generalmente assegnato una volta per tutte al momento della sottoscrizione del servizio e utilizzato per tutte le successive richieste di autenticazione. L'approccio seguito nel GSM/GPRS risolve questo problema variando ad ogni connessione il codice trasmesso.

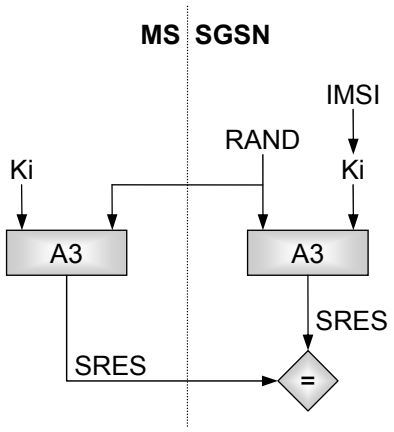

**Figura 7.1.** Metodo di autenticazione del GSM/GPRS

Il principio su cui si basa il processo di autenticazione nel GPRS, come mostrato in Figura 7.1, è di calcolare indipendentemente nella MS e

nell'SGSN una *Signed Response* (SRES) in base alla chiave Ki e ad un particolare numero casuale (RAND) generato di volta in volta dalla rete e comunicato alla MS; se le due SRES coincidono, significa che le due chiavi Ki sono uguali, quindi l'utente è autenticato. Tale procedura ha l'evidente vantaggio di non richiedere la trasmissione della Ki sull'interfaccia radio. L'algoritmo A3 è tale che dalla conoscenza di RAND e SRES (che potrebbero essere intercettati) non è praticamente possibile risalire a Ki: tale operazione è possibile solo in linea di principio, ma è caratterizzata da una complessità computazionale così elevata da richiedere risorse di calcolo di valore maggiore di quello derivante dal possesso illegale della Ki. Inoltre, anche conoscendo un certo numero di coppie (RAND, SRES) legittime, non è possibile risalire al valore corretto di SRES corrispondente a un nuovo valore di RAND.

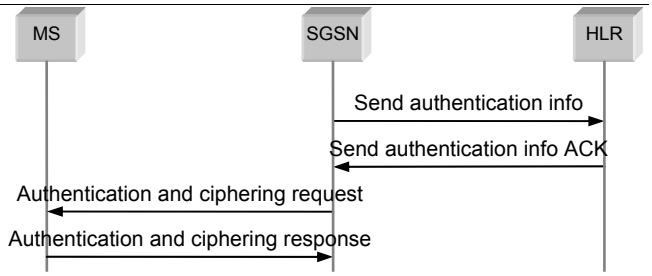


**Figura 7.2.** Processo di autenticazione

Il processo di autenticazione, mostrato in Figura 7.2, prevede dapprima che se il SGSN su cui l'utente intende registrarsi non dispone dei dati per l'autenticazione di quell'utente (Ki, RAND, SRES) li richieda all'HLR[13] mediante un messaggio di SEND AUTHENTICATION INFO in cui è indicato l'IMSI dell'utente di cui necessitano i dati. L'HLR comunica all'SGSN i dati richiesti con un messaggio di SEND AUTHENTICATION INFO ACK. A questo punto, l'SGSN invia alla MS il numero RAND con un messaggio di AUTHENTICATION AND CIPHERING REQUEST. La MS provvede quindi a calcolare la SRES mediante l'algoritmo A3 ed a trasmetterla all'SGSN con un messaggio di AUTHENTICATION AND CIPHERING RESPONSE. Se la SRES ricevuta dalla MS è uguale a quella calcolata o memorizzata dall'SGSN, l'utente è autenticato. In questo modo, i codici scambiati tra MS e SGSN variano ad ogni richiesta di autenticazione e la Ki non viene mai trasmessa sull'interfaccia radio.

## 7.2 Cifratura

L'operazione di cifratura consiste nella sostituzione dei bit di informazione in chiaro con bit cifrati, che (idealmente) dovrebbero costituire una sequenza binaria puramente casuale. In altre parole, la sequenza cifrata dovrebbe essere funzione (invertibile) della sequenza in chiaro, ma tale che dalla sua conoscenza non si possa trarre alcuna informazione sulla sequenza originaria. In pratica, tuttavia, è sufficiente che la complessità computazionale richiesta a una terza parte per risalire ai dati originari sia tale da richiedere un investimento di risorse superiore al valore dell'informazione trasmessa. D'altra parte, è necessario ridurre la complessità dell'operazione di decifratura da parte del destinatario autorizzato, in modo da renderne possibile

[13] Si ricorda (v. par. 2.4) che all'HLR è associato l'*authentication center* (AuC), contenente appunto chiavi e algoritmi utili all'autenticazione degli utenti.

l'esecuzione in tempo reale anche con apparecchiature dalle prestazioni limitate quali le MS. Tali obiettivi possono essere conseguiti utilizzando funzioni invertibili con complessità contenuta nel caso in cui si conosca un'informazione supplementare (la chiave Kc), altrimenti praticamente non invertibili.

Lo standard GPRS prevede che le operazioni di cifratura siano effettuate nello strato LLC tra MS e SGSN; i dati vengono quindi trasmessi in forma cifrata non solo tra MS e BSS (come nel GSM) ma anche tra BSS e SGSN.

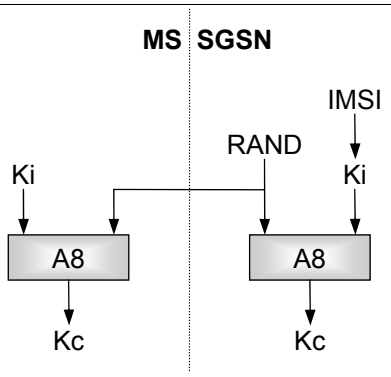


**Figura 7.3.** Calcolo della Kc

Come nel GSM, l'algoritmo A8 genera la chiave Kc a partire dalla Ki e dal numero casuale RAND usato durante la fase di autenticazione (v. Figura 7.3). La Kc è usata quindi per cifrare e decifrare i dati mediante il *GPRS Encryption Algorithm* (GEA).

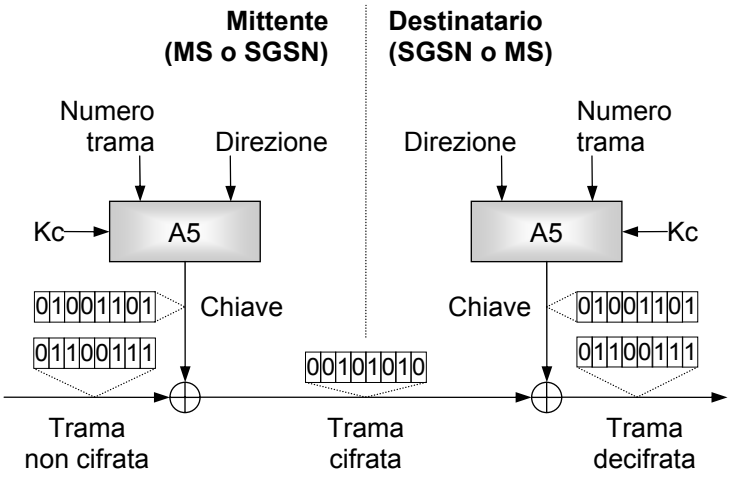


**Figura 7.4.** Cifratura dei dati

Tale algoritmo, definito A5, riceve in ingresso la Kc, un numero dipendente dalla trama LLC corrente e uno dipendente dalla direzione (uplink o downlink), e produce in uscita una chiave, di lunghezza pari a quella di una trama LLC. Al trasmettitore, questa chiave viene sommata modulo 2 bit a bit ai dati contenuti nella trama LLC corrente, generando una trama cifrata. Al ricevitore, analogamente, la stessa chiave è sommata modulo 2 bit a bit alla trama cifrata ricevuta, ottenendo la trama LLC originaria. Le operazioni di cifratura, quindi, avvengono in maniera simmetrica sia nella MS che nell'SGSN: la cifratura e la decifratura sono realizzate utilizzando lo stesso algoritmo e la stessa chiave Kc, calcolata in precedenza. La Figura 7.4 esemplifica questa operazione.

Per risolvere il problema della sincronizzazione dell'istante in cui si iniziano a scambiare messaggi cifrati, è previsto che le operazioni di cifratura e decifratura inizino subito dopo l'invio o la ricezione del messaggio di AUTHENTICATION AND CIPHERING RESPONSE.

## 7.3 Protezione dell'identità dell'utente

Nel GPRS, così come nel GSM, si è provveduto ad assicurare la riservatezza delle informazioni sull'identità dell'utente. Ciò significa che nessuno può scoprire l'identità di chi sta utilizzando una certa risorsa semplicemente esaminando il traffico di segnalazione che transita sul canale radio. Questo permette di mantenere riservati i dati sugli utenti e impedisce di localizzare e di seguire una MS.

Per raggiungere tale scopo, in particolare, l'IMSI non deve mai essere trasmessa in chiaro. Per identificare gli utenti sul canale radio si utilizza perciò, al posto dell'IMSI, una *Packet Temporary Mobile Subscriber Identity* (P-TMSI), analoga alla TMSI del GSM. La P-TMSI è assegnata ad ogni utente dall'SGSN a cui l'utente stesso è collegato in quel momento, ed è valida solo temporaneamente e solo nell'area gestita da quell'SGSN. Per identificare univocamente un utente è quindi necessario indicare sia la P-TMSI che il *Location Area ID* (LAI). L'associazione tra IMSI e P-TMSI è memorizzata solamente nella MS e nell'SGSN. Quando l'utente passa in un'area di traffico gestita da un altro SGSN, viene generata una nuova P-TMSI, comunicata alla MS in forma cifrata.