La crittografia e i difetti della prova per ds

Crittografia è una parola di origine greca che vuol dire “scrittura segreta”; si tratta quindi dell’arte di scrivere messaggi segreti che possano essere letti e compresi solo dal destinatario, mentre per crittoanalisi (dal greco kryptós, “nascosto”, e analýein, “scomporre”) si intende lo studio dei metodi per ottenere il significato di informazioni cifrate. La crittoanalisi si è evoluta di pari passo con la crittografia, infatti, nuovi cifrari venivano introdotti per rimpiazzare quelli violati, e nuove tecniche di crittoanalisi venivano inventate per violare i nuovi schemi. In pratica, sono due facce della stessa medaglia, in altre parole per poter creare una tecnica crittografica sicura bisogna pensarla capace di resistere alla crittoanalisi. Una importante classificazione di tecniche crittografiche è quella che divide la crittografia simmetrica da quella asimmetrica. Per quanto riguarda la prima, uno schema di crittografia simmetrica è quello caratterizzato dalla proprietà che, data la chiave di cifratura “a”, sia facilmente calcolabile la chiave di decifratura “b”. Un caso particolare, spesso utilizzato nella pratica, è l’uso della stessa chiave sia per l’operazione di cifratura che quella di decifratura. La forza della crittografia simmetrica è dunque riposta nella segretezza dell’unica chiave utilizzata dai due interlocutori che la usano e nella resistenza dell’algoritmo agli attacchi di crittoanalisi. Mentre la crittografia asimmetrica è una tecnica crittografica che utilizza chiavi diverse per cifrare e per decifrare un messaggio, facilitando incredibilmente il compito di distribuzione delle chiavi. Infatti in questo caso non è necessario nascondere le chiavi o le password, infatti, esiste una chiave per crittografare, che chiunque può vedere, e una per decifrare, che conosce solo il destinatario senza necessità quindi di riceverla (scambiarla) dal mittente. In altre parole, se A vuole ricevere un messaggio segreto da B, manda a B una scatola vuota con un lucchetto aperto senza chiavi. B mette dentro il messaggio, chiude il lucchetto, e rimanda il tutto ad A, che è l’unico ad avere le chiavi. Chiunque può vedere passare la scatola, ma non gli serve a niente. A non deve correre rischi con le sue chiavi. Oggi chi preleva denaro con il bancomat, chi effettua acquisti su internet con la carta di credito, chi fa una telefonata con il cellulare fa uso, spesso senza rendersene conto, di tecniche crittografiche.

Ma veniamo ora alle schede che saranno consegnate ai 42000 candidati DS alla prova preselettiva del 12 ottobre 2011, da una attenta analisi è possibile dedurre che uno dei punti critici delle schede da consegnare nelle prove, è il numero d’ordine (da 1 a 100), associato alla possibilità di lasciare in bianco tutte le domande che il candidato desideri. Visto che le schede devono essere impersonali, ovvero non è consentito, pena l’esclusione, apporre qualunque segno di riconoscimento sul foglio a lettura ottica o sulle buste, è necessario evitare di rendere efficaci possibili sistemi di identificazione del candidato, associabili alle schede da correggere. In questo contributo si vuole fare un’ipotesi di semplice applicazione crittografica simmetrica riferita a una riconoscibilità numerica che potrebbe rendere labile il

concetto di trasparenza procedurale della prova. Consideriamo che un candidato risponda a sole cinque domande su cento, sovrapponendo sulla scheda i cinque pallini con la penna biro nera. Secondo il numero d'ordine, ipotizziamo che le cinque domande siano: 1, 2, 3, 49, 100, con una somma identificativa di 155, data dalla somma aritmetica dei numeri d'ordine delle cinque domande (1+2+3+49+100 = 155). Il numero 155 è la prima chiave di riconoscibilità, se a questa si aggiunge una seconda chiave, rispondendo, ad esempio, B-A-C-C-A con la seguente sequenza (1-B; 2-A; 3-C; 49-C; 100-A) l'identificazione è certa e soprattutto univoca.

Questa doppia chiave può rendere inutile la presenza della busta piccola dove inserire il nome del candidato e la pratica dei codici a barre atti a garantire l'anonimato. Rimane del tutto evidente che per organizzare una prova preselettiva regolare sia nei contenuti che nella trasparenza, si deve evitare in primo luogo l'errore docimologico e successivamente tutelare l'anonimato del candidato DS in riferimento alle schede da correggere. Nel primo caso è necessaria una competenza disciplinare e docimologica, nel secondo caso una competenza crittoanalitica per neutralizzare le semplici chiavi crittografiche sopra esposte.

Aldo Domenico Ficara