"CHIAVI, LUCCHETTI, BICICLETTE"

(Sceneggiatura da inserire nella puntata sulla crittografia)

Personaggi: I = l'Informatica S = il Sempliciotto P = la Precisina

S: *[Trafelato]* Oh, meno male che siete qui. Ho un problema complicato, ma sono sicuro che voi due genietti mi potete aiutare a risolverlo. Ho un'idea di business fantastica, se mi date una mano sono sicuro che diventeremo ricchi.

P: Tremo già. Come quella volta che hai deciso di investire in borsa basandoti sul tema natale degli amministratori delegati?

S: Seriamente, qui è una cosa grossa. Vi ricordate Hans, quel produttore di biciclette in Engadina? Quello che ho conosciuto alla fiera di orologi a cucù? Stiamo organizzando un business: io ho i miei contatti, raccolgo gli ordini e glieli spedisco. Lui fabbrica le bici, le porta a Chiasso e io le vado a ritirare nel fine settimana, quando sono libero.

P: Da un punto di vista fiscale mi sembra traballante, quest'idea... ma qual è il problema che ti dovremmo aiutare a risolvere?

S: Ecco, si tratta delle chiavi. Fino ad ora, ci regolavamo così: lui comprava dei lucchetti che usava per chiudere le bici a Chiasso, e poi mi spediva le chiavi che io usavo per aprirle. Però questo modo di procedere è un po' rognoso: intanto, c'è il rischio che le chiavi vadano smarrite durante la spedizione, o che qualche postino malintenzionato mangi la foglia e si faccia una copia delle chiavi per poi rubare le bici...

I: Certo: aspettano solo quello, i postini svizzeri.

S: ...e poi avere una chiave per ogni lucchetto è un casino, spesso devo provare tutte le chiavi su tutti i lucchetti prima di capire quale chiave apre quale lucchetto... Insomma, mi servirebbe un modo più semplice e sicuro.

I: E' facilissimo: basta usare il sistema dei lucchetti a combinazione.

S: Cioè?

I: Compri tanti lucchetti a combinazione e li imposti su un numero a tua scelta, che ne so, 19831. Poi li spedisci *aperti* al produttore di biciclette il quale, dopo aver portato le biciclette a Chiasso, le chiude con i lucchetti: tanto mica gli serve la combinazione per chiuderli, giusto? A quel punto solo tu sarai in grado di aprirli e nessun altro. E' l'idea alla base della *crittografia a chiave pubblica*.

P: A “chiave pubblica”?

I: Sì. Nei sistemi crittografici tradizionali, due persone che si vogliano scambiare un messaggio crittato devono prima accordarsi su una “chiave” che viene usata per codificare e decodificare il messaggio; le due persone devono scambiarsi la chiave in modo sicuro, per avere la certezza che nessuno possa carpirla. Questo è il principale punto debole di questi sistemi, che si chiamano *a chiave privata*. Nei sistemi a chiave pubblica, invece, ci sono due chiavi: la chiave di cifratura, che di solito è disponibile a tutti, e quella di decifratura, che è disponibile solo al destinatario.

P: Ah, capisco. E' come dire che un lucchetto a combinazione lo puoi chiudere senza sapere la combinazione, ma per aprirlo la combinazione ti servirà.

I: Sì, l'idea nel caso dei lucchetti si traduce in questo. In informatica, la chiave di cifratura è pubblica e nota a tutti: chi vuole mandarti un messaggio in codice, lo cifra usando la tua chiave pubblica. Per decifrarlo, invece, serve una chiave privata che solo tu hai. Fra l'altro, è sempre su questa idea che si basa il concetto di firma digitale.

S: “Firma digitale”? Ma non è semplicemente la versione scannata della firma di qualcuno?

I: “Scandita”. No, non c'entra niente. La firma digitale è un modo sicuro per garantire

contemporaneamente l'identità del mittente di un messaggio e l'integrità del messaggio stesso. In questo caso, la chiave di cifratura è segreta, mentre quella di decifratura è pubblica, ma l'idea è sempre la stessa.

P: Cioè, se ho capito bene: stavolta la coppia di chiavi è usata in modo diverso; la chiave di codifica è in mano a una persona sola, mentre quella di decodifica è pubblica.

I: Esatto. Ora supponi di voler mandare un messaggio a qualcuno in modo che il destinatario sappia per certo che il messaggio l'hai mandato tu e che non è stato alterato da nessuno. Un modo semplice è questo: conti da quante parole è composto il messaggio, e poi usi la tua chiave di codifica privata per codificare questo numero. Per esempio, se il messaggio è composto da 534 parole, codifichi la parola “Cinquecentotrentaquattro” ottenendo, che ne so, “QWRTSXX”. E metti questa sequenza di caratteri in calce al messaggio. Ci sei?

P: Più o meno...

I: Il destinatario usa la tua chiave pubblica per decodificare la firma e controlla che il valore ottenuto sia il numero di parole del messaggio. Se non è così, o la firma non l'hai apposta tu o il numero di parole è stato alterato... Ricordati che sei l'unico a possedere la chiave di cifratura, quindi l'unico che può codificare correttamente la lunghezza del messaggio.

P: Ingegnoso! Ma se uno modifica il messaggio senza cambiare il numero di parole nessuno se ne può accorgere.

I: Infatti. Per questo motivo si usa qualche metodo più sofisticato per ottenere un sunto del messaggio rendendo la vita più difficile all'eventuale imbroglione.

S: Mi gira la testa!

I: Però dovresti farci l'abitudine. La firma digitale non è solo teoria: anzi, l'Italia è stata uno dei primi Paesi a introdurre la firma digitale equiparandola, di fatto, a una firma autografa! Non sei orgoglioso?

S: Di che?

I: Di essere italiano!