La Vanguardia, 12 de Julio de 2000
ENTREVISTA
PULSO CIUDADANO
MONICA FERNANDEZ Desde sus rudimentarios inicios en la antigüedad hasta sus intrincados sistemas de hoy, la criptografía se ha usado para transmitir mensajes secretos. En nuestra era Internet, se emplea para garantizar la veracidad de los datos.

¿Cómo nació la criptografía?

-Nació durante las guerras de Atenas y Esparta contra Persia y se desarrollaron métodos tan grotescos como cortar el pelo al cero a un esclavo, escribir en su cabeza la información y hacerle correr por las montañas hasta el destino del mensaje, donde llegaba con el pelo ya largo. Allí se le rapaba otra vez y se descubría el mensaje.

-¡Qué método más extraño!

-Se llama esteganografía. Es la manera más rudimentaria de esconder un mensaje, sólo ocultándolo, sin cifrarlo. Los chinos escribían en tela de seda, la doblaban, la recubrían de cera y se la comían. Podemos imaginar como recuperaban el mensaje.

-Mejor no imaginarlo. Sigamos.

-El primero que cifró un mensaje, de manera que aunque se accediera a él no pudiera leerse, porque estaba escrito en código, fue Julio César, para sus campañas militares.

-La criptografía es muy necesaria hoy.

-Sí. Cualquier persona, ya no digamos gobierno o agencia de espionaje, puede acceder con facilidad a un correo electrónico que enviemos. Por eso necesitamos distorsionar los mensajes para que no se sepa qué dicen.

-Da casi miedo.

-Y no es ciencia ficción. Existe el programa Echelon, promovido por los gobiernos de Gran Bretaña, Estados Unidos, Australia y Canadá, que capta millones de conversaciones por teléfono móvil y descubre si incluyen palabras como "bomba", "atentado", "Clinton"... Luego analiza su procedencia.

-Sí, parece que hay problemas con él...

-Si me permite, aprovecho para invitar a todos los que usen el móvil a que incluyan palabras de ese tipo, así les damos trabajo y les fastidiamos.

-Ahí queda la sugerencia. ¿Qué tipo de criptografía se usa hoy en día?

-Cualquier persona puede usar un programa llamado PGP, que se puede descargar de Internet y que cifra los mensajes de correo electrónico. Es indestructible, se basa en una idea matemática muy simple, pero muy brillante. Harían falta siglos de cálculo con un superordenador para descifrarlo. Por esa razón ha tenido problemas legales, está considerado casi un arma en Estados Unidos.

-Aparte de los delincuentes, ¿a quién más le interesa la criptografía?

-A bancos, empresas de venta electrónica... También se usa para crear las firmas digitales y garantizar que la persona que envía un mensaje o hace una compra es quien dice ser y no hay nadie suplantándola.

-¿Toda la criptografía se basa en la matemática?

-Sí. A los matemáticos, lo que nos gusta de la criptografía es que constituye un magnífico ejemplo de cómo una de las ramas más abstractas de la matemática, la teoría de números, algo que parece no tener utilidad, tiene una aplicación importantísima.

-¿Ha descifrado algo complicadísimo?

-(Risas) No. Pero hay una página en Internet del Gobierno británico que ofrece un mensaje cifrado. Quien lo descifre, consigue un trabajo muy bien remunerado en los servicios de inteligencia.