Reverse Engineering of Strong Crypto Signatures Schemes		
Data	by Evilcry	
05/11/2006	UIC's Home Page	**Published by Quequero**
Where ones sees a limit	Qualche mio...eventuale commento sul tutorial :)))	the others sees an opporunity
Prepare for what you cannot see, expect the unexpected, a waiting game waiting to see.....	**WebSite:** http://evilcry.altervista.org **E-mail:** evilcry (GdoG) gmail (GdoG) com (To jump new catching techniques) **IRC frequentato** irc.azzurranet.org #crack-it on efnet #RET	Le radici profonde non gelano mai - Tolkien
Difficoltà	**NewBies** () **Intermedio** (**X**) **Avanzato** (**X**) **Master** ()	

Reverse Engineering of Strong Crypto Signatures Schemes
Written by **Evilcry**.

Introduzione

Ed eccomi qui a scrivere per il NYP2k7 (che più entropicamente contratto non si può), lo stile del paper sarà il classico approccio CryptoRev. Stavolta andremo a trattare principalmente con le ECC ovvero Elliptic Curve Cryptography, con particolare attenzione alle più comuni applicazioni che si trovano nel campo della sicurezza software, ed anche in parte hardware.

Tools usati

- Ida
- Ollydbg
- Buone basi di crittografia e matematica

Indice