HC2 2012 Crypto

(3) Recognizing Plaintexts

You need to know three facts:

a) In Heidi's group Z/pZ, half the elements are quadratic residues, i.e $\exists x$ s.t. $m = x^2 \pmod p$

b) Quadratic residues can be spotted easily, by computing their Legendre symbol $(m|p)$:
$(m|p) = m^{(p-1)/2} \pmod p$

c) We can compute the Legendre Symbol of the cyphertext E from the Symbols of y, F and m

a) With 50% proba, m_1 and m_2 have different Legendre symbols (which means we can detect which one is the right message)

b) Heidi chose her group unwisely! in "real" ElGamal, a group such as integers modulo (p-1)(q-1) is used. Because the Legendre symbol is only defined for integers modulo odd primes, our technique won't work there.

c) $(E|p) = (m \cdot y^r|p) = (m|p) \cdot (g^{xr}|p)$
$(g^{xr}|p)$ is 1 if $(g^x|p)$ is 1
or if $(g^r|p)$ is 1
g^x is y, and g^r is F^{-1} => all known.

(2) Discrete Logarithm

given $g^x \pmod p$, find x

Idea: trade $\sqrt{p}$ time against $\sqrt{p}$ space
Algorithm called "Baby-step, Giant-step"

Write $y=g^x$ as $y=g^{im+j}$, where
m is at least $\sqrt{p}$
i, j range from 0 to m

=> $y \cdot (g^{-m})^i = g^j \pmod p$ for some i, j

Precompute g^j and store them in a hashtable, then try out all possible i.

(1) Decryption

Heidi computes
$E \cdot F^x \pmod p$

This is equivalent to $m \cdot g^{xr} \cdot g^{-xr} = m$

PolyProg

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

open systems

AdNovum