(3) Recognizing Plaintexts

You need to know three facts:

- a) In Heidi's group Z/pZ, half the
 elements are quadratic residues,
 i.e ∃x s.t. m = x² (mod p)
- b) Quadratic residues can be spotted
 easily, by computing their
 Legendre symbol (m|p):
 (m|p) = m^{(p-1)/2} (mod p)
- c) We can compute the Legendre Symbol of the cyphertext E from the Symbols of y, F and m

HC2 2012 Crypto

- 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 (mod 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•F* (mod p)

This is equivalent

to m•g*r•g-xr = m



correct code in C, C++



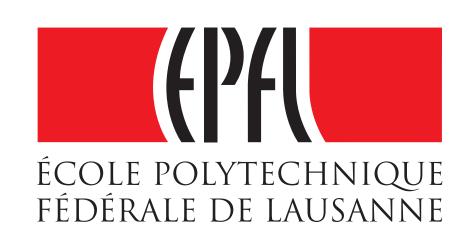
hc2.setDate("March 17, 2012");

hc2.setAttr("fun", "a lot1"):

hc2.timeWarp(3,14192+42/2T);

paceTimeCoord whereAmil(Date to The Theory

hc2. InviteParticipants(STUDENTS, WIGH_SCHOOL, PHD);



Y .

ublic class GregorianCalendar



••••••

