**Malleability and Square Roots**

**Homomorphisms**

The multiplicative homomorphism is f(mn) = f(m)f(n).

RSA has it. E = Mc (mod pq), F = Nc (mod pq) imply EF = (MN)c (mod pq).

This is a weakness in RSA called***Malleability***, which means that the plaintext can be modified, causing a related change in the ciphertext.

The Rabin cryptosystem, E = M2 (mod pq) is especially malleable.

**Square Roots and Factoring**

The ability to find square roots modulo pq confers the ability to factor pq.

**Factoring Algorithm**

1. The square root machine M(x) finds y such that y2 ≡ x (mod pq), given x.

2. Generate random r.

3. Encrypt E = r2 (mod pq). (Rabin encryption)

4. Compute y = M(E). (Rabin decryption.)

5. Compute h = gcd(r+y, pq).

6. If 1 < h < pq, then h ε {p, q}.

**Analysis**

E has 4 square roots modulo pq.

1. (r%p, r%q) 🡨🡪a number ≡ r mod p and ≡ r mod q.

2. ((p-r)%p, r%q)

3.(r%p, (q-r)%q)

4. ((p-r)%p, (q-r)%q).

M(E) will be one of these, each one with probability ¼ .

If M(E) is 1 or 4, we are out of luck.

If M(E) is 2, gcd(r+y, pq) = p.

If M(E) is 3, then gcd(r+y, pq) = q.

We succeed with probability ½ at each iteration. Just repeat until success occurs. The average number of trials needed is 1/( ½ ) = 2.