Rabin cryptosystem.

Step 1: Bob chooses p, q, big primes
$m = p \cdot q$

Step 2: m is published,
p, q kept in secret.

Step 3: Alice encodes the message:
$[t_1, t_2, \dots, t_l]$

Step 4: Alice encrypts the message
$t_i \longrightarrow s_i \equiv t_i^2 \pmod{m}$.

Step 5: Alice sends $[s_1, s_2, \dots, s_l]$ to Bob

Step 6: Bob decrypts the message by solving
$t_i^2 \equiv s_i \pmod{m}$.

Problem: After solving the equation there are 4 solutions and only one of them is correct. It should be guessed somehow.

Attempt to overcome this problem.

Definition: a is called <u>a quadratic residue modulo m</u> if it is a QR modulo p and is a QR modulo q.

Proposition. Let p, q be two distinct primes, $p \equiv q \equiv 3 \pmod{4}$, $m = pq$. Then the following map

$$f : Q_m^\times \longrightarrow Q_m^\times$$
$$a \longmapsto a^2 \pmod m$$

is invertible (i.e. is bijection).

$Q_m^\times := \{a \in \mathbb{Z} : 1 \le a \le m-1,\ \gcd(a,m)=1,\ a \text{ is QR mod } m\}$

Proof.

a is QR mod $p \Longleftrightarrow -a$ is NR mod p

$\left(a^{\frac{p-1}{2}} \equiv 1 \pmod p \right) \Longleftrightarrow (-a)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot a^{\frac{p-1}{2}} \equiv -1 \pmod p)$

Take $a \in Q_m^\times$. $a \equiv u \pmod p$
$a \equiv v \pmod q$

Then for $b = f(a)$ we have

$b \equiv u^2 \pmod p$

$b \equiv v^2 \pmod q$

The preimage of b is contained in the following set: $\{(\pm u \pmod p), \pm v \pmod q)\}$.

It contains only one quadratic residue, namely $(u \pmod p), v \pmod q))$. $\boxtimes$

Note: The inverse of f can be computed as follows:

$$\begin{pmatrix} u \pmod p \\ v \pmod q \end{pmatrix} \xrightarrow{f^{-1}} \begin{pmatrix} u^{\frac{p+1}{4}} \pmod p \\ v^{\frac{q+1}{4}} \pmod q \end{pmatrix}.$$

Problem: We need to publish some knowledge about Q_m^x, but that will give too much information. Even a method which checks whether a is inside Q_m^x or not, gives too much information.