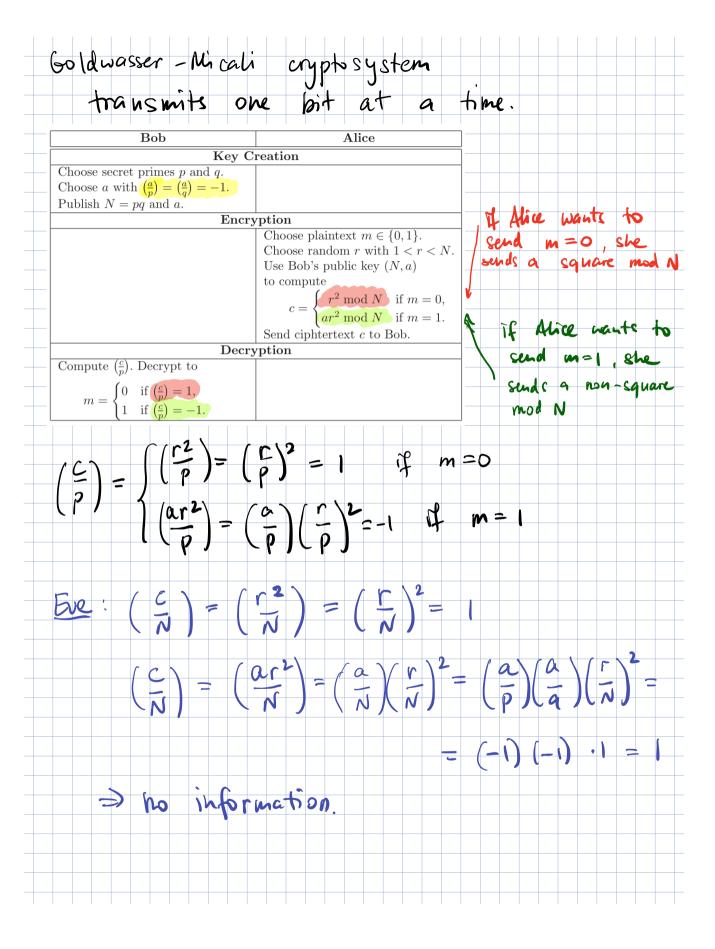
3.10. Probabilist	ne Encrypt	on.	
In any PKC	if the set	of possible	plaintexts
(using Bob's p	ublic key)	and compa	Ide cipher texts re the list
to Alice's ci			
Probabilistic Abstract idea:	encry phon	is a way	around this issue:
. Alice has	a plaintext	m	
Chooses 9	random st	ning of da	ta p
	the pair (m,		
based on	the follow	ing problem	ntosystem (GMCS)
let p,q be	two prime	es and 1	V = pq
For a \ \ \ \ mod \ N.	determne	whether a	is a square
Bob (knows p	and g).	Eve (das	not know p and q)
a is a ja	- (a)	(a) = 1	- no infa
square (=) (p)	9)=(



Example Bob:
$$p = 23$$
, $q = 17 - \text{secret}$
 $N = pq = 391$
 $a = 3$

$$\begin{pmatrix} \frac{3}{2} \\ \frac{3}{2} \end{pmatrix} = \begin{pmatrix} \frac{13}{2} \\ \frac{3}{2} \end{pmatrix} = \begin{pmatrix} \frac{2}{3} \\ \frac{3}{2} \end{pmatrix} = -1$$

Alice enact to send $m = 0$
· chooses a random $r = 281$
· sends ciphertext $c = r^2 \mod N = 370 \pmod{39}$

Bub: $\left(\frac{370}{23}\right) = \begin{pmatrix} \frac{2}{23} \end{pmatrix} = 1 \implies m = 0$

Note: • GMCS is not practical because if N has 1000 bits then the message expansion ratio is 1000.

• But probabilistic ideas (introducing a vandom element) make PEC more secure.
• It is desirable to take deterministic PEC (such as RSA) and turn them into probabilistic oves