Ralph's quantum encryption

Ralph wishes to send secure messages and realizes that classical approaches (RSA and elliptical curve cryptography) are vulnerable to quantum computation. However, private key encryption using quantum cryptography to send the key is fundamentally secure. The sender's key e and prime modulus p are privately shared via quantum encryption utlizing, say, binary code.[1]

decimal	binary	decimal	binary
0	00000	16	10000
1	00001	17	10001
2	00010	18	10010
3	00011	19	10011
4	00100	20	10100
5	00101	21	10101
6	00110	22	10110
7	00111	23	10111
8	01000	24	11000
9	01001	25	11001
10	01010	26	11010
11	01011	27	11011
12	01100	28	11100
13	01101	29	11101
14	01110	30	11110
15	01111	31	11111

The spirit of quantum encryption is reflected in the following.

1. Ralph (sender) randomly chooses between standard and Hadamard basis where 0 is represented by $|0\rangle$ and $H|0\rangle = |+\rangle$, respectively, and 1 is represented by $|1\rangle$ and $H|1\rangle = |-\rangle$, respectively.

2. Alice (receiver) chooses to measure in either standard or Hadamard basis and communicates the choice to Ralph where the observables $Z = 1|0\rangle\langle 0| - 1|1\rangle\langle 1|$ and $X = 1|+\rangle\langle +| - 1|-\rangle\langle -|$ perform the measurement. If the basis choice matches Ralph's choice then Ralph instructs Alice to keep the result. If the basis choice does not match, the result is discarded and another qubit from a randomly chosen basis transmitted. If the measurement result from Z or X is 1 then 0 is received. Alternatively, if the measurement result from Z or X is -1 then 1 is received.

3. After sufficient binary strings have been matched to convey private keys e and p, Alice prepares a decoder d that satisifes $ed \equiv 1 \bmod (p-1)$.

4. A test message m is encoded $em \equiv m^e \bmod p$, transmitted, decoded $m' \equiv em^d \bmod p$ and checked $m = m'$. If Eve (eavesdropper) has intercepted

[1] For purposes of illustration we use small numbers but in practice much larger and randomly selected numbers can be quickly transmitted.

the communication she will almost surely have changed the state (qubit). Even if there is a chance match the keys will almost surely be corrupted and test message will fail. Then, the process begins anew.

If $|0\rangle$ or $H|0\rangle = |+\rangle$ is sent and matched by the receiver the qubit indicates a 0 in the binary string. Alternatively, if $|1\rangle$ or $H|1\rangle = |-\rangle$ is sent and matched by the receiver the qubit indicates a 1 in the binary string. For instance, the matched string $|0\rangle$,$|+\rangle$, $|+\rangle$, $|-\rangle$,$|1\rangle$ is binary code for 3.

Suppose Ralph chooses $(e = 3, p = 11)$, uses binary strings to encode via the basis for observables Z, X, X, Z, Z, Z, X, X then repeats (as necessary) and employs a test message $m = 32$ (one digit at-a-time), Eve employs measurements Z, I, I,X then repeats (I is the identity matrix and implies no interference), and Alice uses measurements Z, Z, X, X then repeats.[2]

Suggested:

1. Create a table identifying matched measurement bases for Ralph and Alice, qubits (and possibly messages) effectively intercepted by Eve, and the number of cycles required to effectively communicate the private keys e and p (in binary format) and the message m (in decimal format). If there is positive probability the key is corrupted try all possibilities to enumerate the odds of successful transmission of the private key. If Alice's received key p' for p is not prime then she tries the next prime number.

Hint: Use Fermat's theorem and private key encryption to encode and decode m (in decimal format rather than binary).

$$a^p \equiv a \bmod p$$

$$a^{p-1} \equiv 1 \bmod p$$

$$a^{ed} = a^{(p-1)n+1} \equiv a \bmod p$$

$$ed = (p-1)\,n + 1$$

$$ed \equiv 1 \bmod (p-1)$$

$$m^e \equiv m' \bmod p$$

$$m'^d = m^{ed} \equiv m \bmod p$$

After private keys e and p are received by Alice. Alice determines d from the third to last line above, Ralph encodes m via the second to last line above, and Alice decodes the received message m' by the last line above.

2. Repeat 1 where everything is the same except Eve's measurements are X, I, Z repeated.

[2] In practice, measurement bases as well as private keys are randomized.