

COIN FLIPS BY TELEPHONE

(Taken from Trappe and Washington.)

Alice chooses two large primes p and q , both 3 mod 4, computes their product n , and sends n to Bob.

Bob computes some random square modulo n , $y = x^2 \% n$, and sends it to Alice.

Alice computes

$$z_p = y^{(p+1)/4} \% p.$$

In fact, $\pm z_p \% p$ are the square roots of y modulo p . One proof of this fact is that the fourth power of $\pm z_p$ is $y^{p+1} = y^2$ (working modulo p), and so their square is $\pm y$. But because p is a 3 mod 4 prime, not both of $\pm y$ can be squares, and so $z_p^2 = y$. A nicer proof is that in general,

$$\eta^{(p-1)/2} \% p = \begin{cases} 1 & \text{if } \eta \text{ is a square modulo } p, \\ -1 & \text{if not.} \end{cases}$$

(This follows from the cyclic structure of $(\mathbf{Z}/p\mathbf{Z})^\times$.) In particular, $y^{(p-1)/2} = 1$, and so

$$z_p^2 = y^{(p+1)/2} = y^{1+(p-1)/2} = y \quad (\text{working modulo } p).$$

In any case, Alice similarly computes

$$z_q = y^{(q+1)/4} \% q,$$

a square root of y modulo q . So, Alice knows the square roots of $(y \% p, y \% q)$ in $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$: they are

$$(\pm z_p, \pm z_q) \quad \text{where the two “}\pm\text{” signs are independent.}$$

This information passes back through the Sun Ze isomorphism

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z}),$$

so that Alice knows the four square roots of y in $\mathbf{Z}/n\mathbf{Z}$. Call them

$$\pm w, \quad \pm \tilde{w}.$$

One of the pairs here includes the x that Bob used to compute $y = x^2 \% n$ in the first place. But Alice doesn't know which pair it is.

Alice guesses one of her pairs, say $\pm w$, and sends it to Bob. If her pair includes x then she has won the coin flip. If not, then she has lost.

The point here is that if Bob claims that Alice has lost the coin flip, then Bob is claiming that in light of the information that she sent him, he now knows all four square roots $\{\pm w, \pm \tilde{w}\}$ of y modulo n , and therefore he is claiming that he can factor n . Indeed, he can compute

$$\gcd(w - \tilde{w}, n),$$

and this is a nontrivial factor of n . To see this, note that

$$w^2 - \tilde{w}^2 = 0 \pmod n,$$

which is to say that

$$(w - \tilde{w})(w + \tilde{w}) = 0 \pmod{p} \quad \text{and} \quad (w - \tilde{w})(w + \tilde{w}) = 0 \pmod{q}.$$

Thus $w - \tilde{w}$ is divisible by one of p, q , otherwise $w - \tilde{w}$ would have to be divisible by them both.