The Rabin-Miller Test — Examples

n = 252601, $n-1 = 2^3 \cdot 31575$.
Choose $a = 85132$.

$$a^{31575} \equiv 191102 \pmod{n}$$
$$a^{2\cdot 31575} \equiv 184829 \pmod{n}$$
$$a^{2^2\cdot 31575} \equiv 1 \pmod{n}$$

Conclusion: n is ***composite***. (184829 is a square root of 1, mod n, different from ±1.)

n = 3057601, $n-1 = 2^6 \cdot 47775$.
Choose $a = 99908 \pmod{n}$.

$$a^{47775} \equiv 1193206 \pmod{n}$$
$$a^{2\cdot 47775} \equiv 2286397 \pmod{n}$$
$$a^{2^2\cdot 47775} \equiv 235899 \pmod{n}$$
$$a^{2^3\cdot 47775} \equiv 1 \pmod{n}$$

Conclusion: n is ***composite***. (235899 is a square root of 1, mod n, different from ±1.)

n = 104717, $n-1 = 2^2 \cdot 26179$.
Choose $a = 96152$.

$$a^{26179} \equiv 1 \pmod{n}$$

Conclusion: n is ***probably prime***.

n = 577757, $n-1 = 2^2 \cdot 144439$.
Choose $a = 314997 \pmod{n}$.

$$a^{144439} \equiv 373220 \pmod{n}$$
$$a^{2\cdot 144439} \equiv 577756 \equiv -1 \pmod{n}$$

Conclusion: n is ***probably prime***.

n = 101089, $n-1 = 2^5 \cdot 3159$.
Choose $a = 5$.

$$a^{3159} \equiv 101088 \equiv -1 \pmod{n}$$

Conclusion: n is ***probably prime***.

n = 280001, $n-1 = 2^6 \cdot 4375$.
Choose $a = 105532$.

$$a^{4375} \equiv 236926 \pmod{n}$$
$$a^{2\cdot 4375} \equiv 168999 \pmod{n}$$
$$a^{2^2\cdot 4375} \equiv 280000 \equiv -1 \pmod{n}$$

Conclusion: n is ***probably prime***.

$\boldsymbol{n} = \mathbf{95721889}$, $n-1 = 2^5 \cdot 2991309$.

Choose $a = 21906436$.

$$a^{2991309} \equiv 373440 \pmod{n}$$
$$a^{2 \cdot 2991309} \equiv 86363216 \pmod{n}$$
$$a^{2^2 \cdot 2991309} \equiv 93382930 \pmod{n}$$
$$a^{2^3 \cdot 2991309} \equiv 31803553 \pmod{n}$$
$$a^{2^4 \cdot 2991309} \equiv a^{(n-1)/2} \equiv 63099174 \pmod{n}$$

Conclusion: n is ***composite***.

(If $\left(a^{(n-1)/2}\right)^2 \equiv a^{n-1} \equiv 1 \pmod{n}$, then $a^{(n-1)/2} \equiv 63099174 \pmod{n}$ is a square root of 1, different from ±1. Otherwise Fermat's Little theorem implies that n is composite.)