Solutions to Daily Due Sep 25 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

*Conventions as in lecture: for Miller-Rabin, write $n-1 = 2^k m$ with m odd and compute the chain $a^m \to a^{2m} \to \cdots \to a^{2^k m} = a^{n-1}$ modulo n, each term the square of the one before. Then n is **composite** if (a) the chain never reaches 1, or (b) a term other than ± 1 squares to 1 (an "unusual" square root of 1). Otherwise n is **probably prime**.*

Problems 1 and 2: Miller-Rabin on $n = 90751$

$n - 1 = 90750 = 2 \cdot 45375$, so $k = 1$ and $m = 45375$. The chain has just two terms.

$a = 2$**:** $2^{45375} \equiv 1 \pmod{90751}$. The chain is $1 \to 1$: it reaches 1 and there is no unusual square root. Verdict: **probably prime**.

$a = 3$**:** $3^{45375} \equiv 30652 \pmod{90751}$, and $30652^2 \equiv 1$. The chain is $30652 \to 1$. So 30652 is a square root of 1 that is not ± 1 (note $-1 \equiv 90750$). Verdict: **composite**.

In fact the unusual square root hands us a factor, as on the "surfeit of square roots" slide: $\gcd(30652 - 1, 90751) = 601$, so

$$90751 = 151 \cdot 601.$$

So 2 was a *liar* for 90751, and 3 was a *witness*. Note that $3^{90750} \equiv 1$, so the Fermat test with base 3 would also have been fooled; it is the square-root check that catches n.

Problem 3: Miller-Rabin on $n = 3057601$ with $a = 99908$

$n - 1 = 3057600 = 2^6 \cdot 47775$, so $k = 6$ and $m = 47775$. The chain is

$$99908^{47775} \equiv 1193206 \;\to\; 2286397 \;\to\; 235899 \;\to\; 1 \;\to\; 1 \;\to\; 1 \;\to\; 1 \pmod{3057601}.$$

The term 235899 squares to 1 but is not ± 1. Verdict: **composite**.

Again the gcd splits n: $\gcd(235899 - 1, n) = 9073 = 43 \cdot 211$ and $\gcd(235899 + 1, n) = 337$, so

$$3057601 = 43 \cdot 211 \cdot 337.$$

This n is a **Carmichael number**: 42, 210 and 336 all divide $n-1$, so $a^{n-1} \equiv 1$ for *every* a coprime to n and the Fermat test can never detect it. Miller-Rabin does.

Problem 4: Fermat factoring $n = 16080$

Look for y with $n + y^2$ a perfect square, trying $y = 1, 2, 3, \ldots$:

y	$n + y^2$	square?
1	16081	no ($126^2 = 15876,\ 127^2 = 16129$)
2	16084	no
3	16089	no
4	16096	no
5	16105	no
6	16116	no
7	16129	yes: 127^2

So $16080 = 127^2 - 7^2 = (127 - 7)(127 + 7) = 120 \cdot 134$. (Fully factored, $16080 = 2^4 \cdot 3 \cdot 5 \cdot 67$; of course, being even, it did not really need Fermat!)

Problem 5: factoring $n = 38191$ from the given relations

Each relation says $k^2 \equiv$ (a factored number) $\pmod{n}$. Record the exponent vectors, with one entry for each of the primes 2, 3, 5, 13, 17, 19:

k	$k^2 - n$	$(2, 3, 5, 13, 17, 19)$
196	$3^2 \cdot 5^2$	$(0, 2, 2, 0, 0, 0)$
201	$2 \cdot 5 \cdot 13 \cdot 17$	$(1, 0, 1, 1, 1, 0)$
214	$3^2 \cdot 5 \cdot 13^2$	$(0, 2, 1, 2, 0, 0)$
227	$2 \cdot 3^3 \cdot 13 \cdot 19$	$(1, 3, 0, 1, 0, 1)$
229	$2 \cdot 3 \cdot 5^3 \cdot 19$	$(1, 1, 3, 0, 0, 1)$
241	$2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17$	$(1, 2, 1, 1, 1, 0)$
254	$3^4 \cdot 5^2 \cdot 13$	$(0, 4, 2, 1, 0, 0)$

We want a set of rows whose vectors add up to all even entries.

A single row. Row 196 is already all even: $196^2 \equiv 15^2 \pmod{n}$. Then $\gcd(196 - 15, n) = \gcd(181, 38191) = 181$.

A pair (the intended combination). Rows 201 and 241 add to $(2, 2, 2, 2, 2, 0)$:

$$(201 \cdot 241)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 13 \cdot 17)^2, \qquad x = 201 \cdot 241 \equiv 10250, \quad y = 6630.$$

Then $\gcd(10250 - 6630, n) = \gcd(3620, 38191) = 181$.

Either way,

$$38191 = 181 \cdot 211.$$

A trap: combining all three rows $196, 201, 241$ is also all even, but gives $x \equiv y \equiv 23068$, so $\gcd(x - y, n) = n$: a trivial factorization. Not every even combination works; if one fails, try another.

Problem 6: factoring 21733 from $\varphi(21733) = 21420$

If $n = pq$ then $\varphi(n) = (p-1)(q-1) = n - (p+q) + 1$, so

$$p + q = n - \varphi(n) + 1 = 21733 - 21420 + 1 = 314, \qquad pq = 21733.$$

So p, q are the roots of $z^2 - 314z + 21733 = 0$. The discriminant is $314^2 - 4 \cdot 21733 = 98596 - 86932 = 11664 = 108^2$, so

$$z = \frac{314 \pm 108}{2} = 211 \text{ or } 103, \qquad 21733 = 103 \cdot 211.$$

Moral: knowing $\varphi(n)$ is as good as knowing the factorization of an RSA modulus.

Problems 7 and 8: quadratic sieve for $n = 31861$

Here $\lfloor \sqrt{n} \rfloor = 178$, so we sieve $k = 179, 180, \ldots$. The useful primes are 2 and the odd primes q for which n is a square modulo q; up to 29 these are $\{2, 3, 5, 7, 11, 19, 23\}$. (The tool's factor base and relations will vary; this is one run.) Some k with $k^2 - n$ smooth:

k	$k^2 - n$	factored
179	180	$2^2 \cdot 3^2 \cdot 5$
180	539	$7^2 \cdot 11$
181	900	$2^2 \cdot 3^2 \cdot 5^2$
184	1995	$3 \cdot 5 \cdot 7 \cdot 19$
196	6555	$3 \cdot 5 \cdot 19 \cdot 23$
241	26220	$2^2 \cdot 3 \cdot 5 \cdot 19 \cdot 23$
260	35739	$3^2 \cdot 11 \cdot 19^2$
269	40500	$2^2 \cdot 3^4 \cdot 5^3$

Lucky single relation (Problem 7). $181^2 - n = 900 = 30^2$ is already a square, so $\gcd(181 - 30, n) = 151$. (This is just Fermat factoring: $n = 181^2 - 30^2 = 151 \cdot 211$.)

Combinations (Problem 8).

- $k = 180, 260$: $539 \cdot 35739 = 3^2 \cdot 7^2 \cdot 11^2 \cdot 19^2$. So $x = 180 \cdot 260 \equiv 14939$, $y = 3 \cdot 7 \cdot 11 \cdot 19 = 4389$, and $\gcd(14939 - 4389, n) = \gcd(10550, 31861) = 211$.
- $k = 196, 241$: $6555 \cdot 26220 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 19^2 \cdot 23^2$. So $x = 196 \cdot 241 \equiv 15375$, $y = 2 \cdot 3 \cdot 5 \cdot 19 \cdot 23 = 13110$, and $\gcd(15375 - 13110, n) = \gcd(2265, 31861) = 151$.
- $k = 179, 269$: $180 \cdot 40500 = 2^4 \cdot 3^6 \cdot 5^4$. So $x = 179 \cdot 269 \equiv 16290$, $y = 2^2 \cdot 3^3 \cdot 5^2 = 2700$, and $\gcd(16290 - 2700, n) = 151$.

In every case,

$$31861 = 151 \cdot 211.$$

Problem 9: the small-message attack on the ciphertext chain

The specific ciphertexts live on the #ciphertexts channel, so here is the method. Suppose $c \equiv m^e \pmod{n}$ and the message is short, say $m < 2^B$. If $m = xy$ with x, y both at most about $2^{B/2}$ (this happens with reasonable probability), then

$$c \cdot x^{-e} \equiv y^e \pmod{n}.$$

1. Make a list of $y^e \bmod n$ for $y = 1, 2, \ldots, Y$.
2. Make a second list of $c \cdot x^{-e} \bmod n$ for $x = 1, 2, \ldots, X$.
3. Look for a value on both lists (a collision). Then $m = xy$; check by computing $(xy)^e \equiv c$.

With $X, Y \approx 2^{B/2}$ this is about $2^{B/2}$ work instead of 2^B for trying every message: the same square-root speedup as the birthday attack and baby-step giant-step. A message of a few letters (say $B \approx 30$ bits) falls in about $2^{15} \approx 33{,}000$ steps. The defence, as in class: **pad short messages** with random bits before encrypting. See the `RSA short plaintext` tool and textbook Section 3.6.3.

Problem 10 (optional): Carmichael numbers

A Carmichael number is a composite n with $a^{n-1} \equiv 1 \pmod{n}$ for every a coprime to n. A short Sage search:

```
for n in range(3, 10000, 2):
    if not is_prime(n) and all(power_mod(a, n-1, n) == 1
                               for a in range(2, n) if gcd(a, n) == 1):
        print(n, factor(n))
```

finds

$$561 = 3 \cdot 11 \cdot 17, \quad 1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19, \quad 2465,\ 2821,\ 6601,\ 8911.$$

Korselt's criterion explains them: n is Carmichael exactly when it is squarefree and $p - 1 \mid n - 1$ for every prime $p \mid n$ (e.g. for 561: $2, 10, 16$ all divide 560). The number 3057601 from Problem 3 is another one.