Solutions to Daily Due Sep 4 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(follows the Diffie-Hellman setup of the Fall 2024 lecture notes of Sept 9;
all computations computer-verified)

The daily post was an exercise rather than a problem set: perform a Diffie-Hellman key exchange on discord and use the shared secret to send a short message. Everyone's numbers are different, so here is one complete worked example with every number written out, in the order of the steps in the post. You can paste any of these numbers into the *Text to Integer* and *Diffie-Hellman Tools* pages to check them.

The public setup (step 4.3)

Everyone shares the prime and the primitive root:

$$p = 10^{15} + 37 = 1000000000000037, \qquad g = 2.$$

(Both facts were given to us; a computer confirms them: p is prime, $p-1 = 2^2 \cdot 7 \cdot 37 \cdot 965250965251$, and $2^{(p-1)/q} \not\equiv 1 \pmod{p}$ for each prime q dividing $p-1$, so 2 has multiplicative order $p-1$.)

Alice's message (steps 4.1–4.2)

Say Alice answers "Why CU?" with the six characters `Buffs!`. The *Text to Integer* tool writes each character as its ASCII code,

$$\texttt{B} = 66, \quad \texttt{u} = 117, \quad \texttt{f} = 102, \quad \texttt{f} = 102, \quad \texttt{s} = 115, \quad \texttt{!} = 33,$$

and reads these as the digits of an integer in base 255, *first character least significant*:

$$m = 66 + 117 \cdot 255 + 102 \cdot 255^2 + 102 \cdot 255^3 + 115 \cdot 255^4 + 33 \cdot 255^5 = 36068675793951.$$

Six characters give at most $255^6 \approx 2.7 \times 10^{14} < p$, which is why the message had to be short: it must be a residue modulo p.

Alice's keys (steps 4.4–4.6)

Alice picks a random secret key

$$a = 224150560099795$$

and announces her public key on #public-keys:

$$A \equiv g^a = 2^{224150560099795} \equiv 246319747102364 \pmod{p}.$$

(Successive squaring: about 48 squarings and at most 48 multiplications, all modulo p; this is what the third box of the tools page does.)

Bob's keys (step 4.7)

Bob did the same with his own secret b and posted

$$B \equiv g^b \equiv 11667749654898 \pmod{p}.$$

For the record (Alice never learns this), Bob's secret was $b = 316377587606637$.

The shared secret (step 4.7)

Alice raises Bob's public key to her secret exponent; Bob raises Alice's public key to his. They get the same number because both are g^{ab}:

$$s \equiv B^a \equiv A^b \equiv g^{ab} \equiv 425644724809256 \pmod{p}.$$

Encrypting (step 4.8)

Alice adds the shared secret to her message modulo p and posts the result on #ciphertexts as the secret message for Bob:

$$\begin{aligned} c \equiv m + s &= 36068675793951 + 425644724809256 \\ &= 461713400603207 \pmod{p}. \end{aligned}$$

(No reduction was needed here since the sum is less than p; in general one reduces.)

Decrypting (step 4.9)

Bob computes the shared secret $s = A^b \bmod p = 425644724809256$ from Alice's public key and his own secret, subtracts it,

$$\begin{aligned} m \equiv c - s &= 461713400603207 - 425644724809256 \\ &= 36068675793951 \pmod{p}, \end{aligned}$$

and feeds 36068675793951 to the *Integer to Text* box, which recovers the base-255 digits 66, 117, 102, 102, 115, 33, that is, `Buffs!`.

What an eavesdropper sees

Everything on discord is public: p, g, $A = g^a$, $B = g^b$, and $c = m + g^{ab}$. To read m the eavesdropper needs g^{ab} (the computational Diffie-Hellman problem), and the only known route is to find a from A or b from B (the discrete logarithm problem). With a 16-digit prime that is within reach of the algorithms coming up next (baby-step giant-step and its relatives), which is exactly why the next daily post invites you to try breaking one of the class ciphertexts, and why real Diffie-Hellman uses primes of hundreds of digits.