

Q1 *Cryptography: EvanCRHF*

(24 points)

EvanBot is designing a hash function $H : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$.

Notation for the entire question:

- 0^n is an n -bit bitstring of all zeros.
- $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is a one-way, collision-resistant hash function (CRHF).

For each subpart with boxes, select whether the function is a CRHF.

- If “Yes,” leave the boxes blank.
- If “No,” give a collision pair $(x_1, x_2), (y_1, y_2)$ such that $H(x_1, x_2) = H(y_1, y_2)$ and $(x_1, x_2) \neq (y_1, y_2)$.

Example: If $H(a, b) = a + b$, then a valid solution is $(x_1, x_2) = (2, 3), (y_1, y_2) = (4, 1)$.

Assumptions:

- x_1, x_2, y_1, y_2 are exactly n bits each, but you may answer with a simple integer and assume it is converted to the associated bitstring.
- There may be multiple correct answers. In the example above, $(x_1, x_2) = (1, 9), (y_1, y_2) = (5, 5)$ would also be correct.

Q1.1 (3 points) Is $H(a, b) = a \| f(b)$ a CRHF?

- ☐ Yes (leave the boxes blank) ☐ No (fill in the boxes)

$x_1 :$		$x_2 :$	
$y_1 :$		$y_2 :$	

Q1.2 (3 points) Does $H(a, b) = a \| f(b)$ possess one-wayness?

- ☐ Yes, because an attacker must still invert $f(b)$ to find the complete pre-image (a, b) .
- ☐ Yes, because it is computationally difficult to determine where a ends and $f(b)$ begins.
- ☐ No, because the first part of the input (a) is leaked directly in the output.
- ☐ No, because the output length is strictly greater than the input length.



(Question 1 continued...)

Q1.3 (3 points) Is $H(a, b) = 0^n \| f(a)$ a CRHF?

- ☐ Yes (leave the boxes blank) ☐ No (fill in the boxes)

$x_1 :$		$x_2 :$	
$y_1 :$		$y_2 :$	

Q1.4 (3 points) Does $H(a, b) = 0^n \| f(a)$ possess one-wayness?

- ☐ Yes, because fixing the first n bits prevents collisions across different inputs, which is enough to make it one-way.
- ☐ Yes, because an attacker still needs to invert $f(a)$ to find a valid a for the pre-image.
- ☐ No, because the construction leaks b directly in the output, so inverting is trivial by reading b .
- ☐ No, because the output only covers strings with prefix 0^n , so the function cannot be one-way for all outputs.

For the following **two subparts**, let the hash function from Q1.3 be G , so $G(a, b) = 0^n \| f(a)$.

Q1.5 (3 points) Is $H(a, b) = G(G(a, b))$ a CRHF?

Note: The output of G is a $2n$ bit string. By splitting this in half, it is possible to produce a tuple of form (a, b) that can serve as the input to G .

- ☐ Yes (explain your answer below) ☐ No (explain your answer below)

Why or why not? Use 10 words or fewer (the staff answer is 5 words).

Q1.6 (3 points) Does $H(a, b) = G(G(a, b))$ possess one-wayness?

- ☐ Yes, because a is not used to compute the output $H(a, b)$.
- ☐ Yes, because b is not used to compute the output $H(a, b)$.
- ☐ No, because the output is a constant for all inputs, making inversion trivial.
- ☐ No, because the output length is smaller than the input length, which always breaks one-wayness.

(Question 1 continued...)

For the **remaining subparts**, EvanBot is attempting to design CRHF $H : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n$ that outputs n -bit strings.

Q1.7 (3 points) Is $H(a, b) = a \oplus b \oplus f(a \oplus b)$ a CRHF?

☐ Yes (leave the boxes blank) ☐ No (fill in the boxes)

$x_1 :$		$x_2 :$	
$y_1 :$		$y_2 :$	

Q1.8 (3 points) Is $H(a, b) = a^b \bmod p$ a CRHF?

Assume that a and b are cast to integers, and then the resulting integer $a^b \bmod p$ is cast back to an n -bit string.

☐ Yes (leave the boxes blank) ☐ No (fill in the boxes)

$x_1 :$		$x_2 :$	
$y_1 :$		$y_2 :$	