Cryptography – Endterm

Last name: Eck

First name: Anne

Student ID no.:

Signature:

- If you feel ill, let us know immediately.
- Please, **do not write** until told so.
- You will be given **120 minutes** to fill in all the required information and write down your solutions.
- Don't forget to **sign**.
- Write with a non-erasable **pen**, do not use red or green color.
- You are not allowed to use **auxiliary means** other than your pen and a simple calculator.
- You may answer in **English or German**.
- Please turn off your **cell phone**.
- Check that you have received **15 sheets of paper** and, please **do not destroy the binding**.
- Write your **solutions** directly into the exam booklet.
- Should you require additional **scrap paper**, please tell us.
- You can obtain **40 points** in the exam. You need **17 points** in total to pass (grade 4.0). The bonus applies only if you pass the exam.
- See the next page for a list of **abbreviations**.
- Don't fill in the table below.
- Good luck!

Ex1	Ex2	Ex3	Ex4	Ex5	Ex6	$\sum$

Abbreviations

- RO = random oracle
- RPO = random permutation oracle
- OWF = one-way function (family/collection)
- OWP = one-way permutation (family/collection)
- TDP = trapdoor one-way permutation
- PRG = pseudorandom generator
- PRF = pseudorandom function
- PRP = pseudorandom permutation
- TBC = tweakable block cipher
- UOWHF = universal one-way hash function (family/collection)
- CRHF = collision resistant hash function (family/collection)
- ES = (private-key) encryption scheme
- PKES = public-key encryption scheme
- MAC = message authentication code
- DSS = digital signature scheme
- DLP = discrete logarithm problem
- CDH = computational Diffie-Hellman problem
- DDH = decisional Diffie-Hellman problem
- $\oplus$ = bitwise XOR

Exercise 1 **6P**

Draw a directed graph with nodes

(A) computationally secret ES with $|\mathcal{K}| < |\mathcal{M}|$ exist
(B) RSA problem is hard w.r.t. $\mathsf{Gen}\mathbb{P}^2$
(C) $\mathbf{NP} \neq \mathbf{P}$ holds
(D) PRG of variable stretch exist
(E) CCA-secure ES exist
(F) OWP exist
(G) DDH is hard w.r.t. $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$
(H) OWF exist
(I) PRF of key and block length n exist
(J) CDH is hard w.r.t. $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$
(K) CRHF with sufficient compression exist
(L) CCA-secure PKES exist

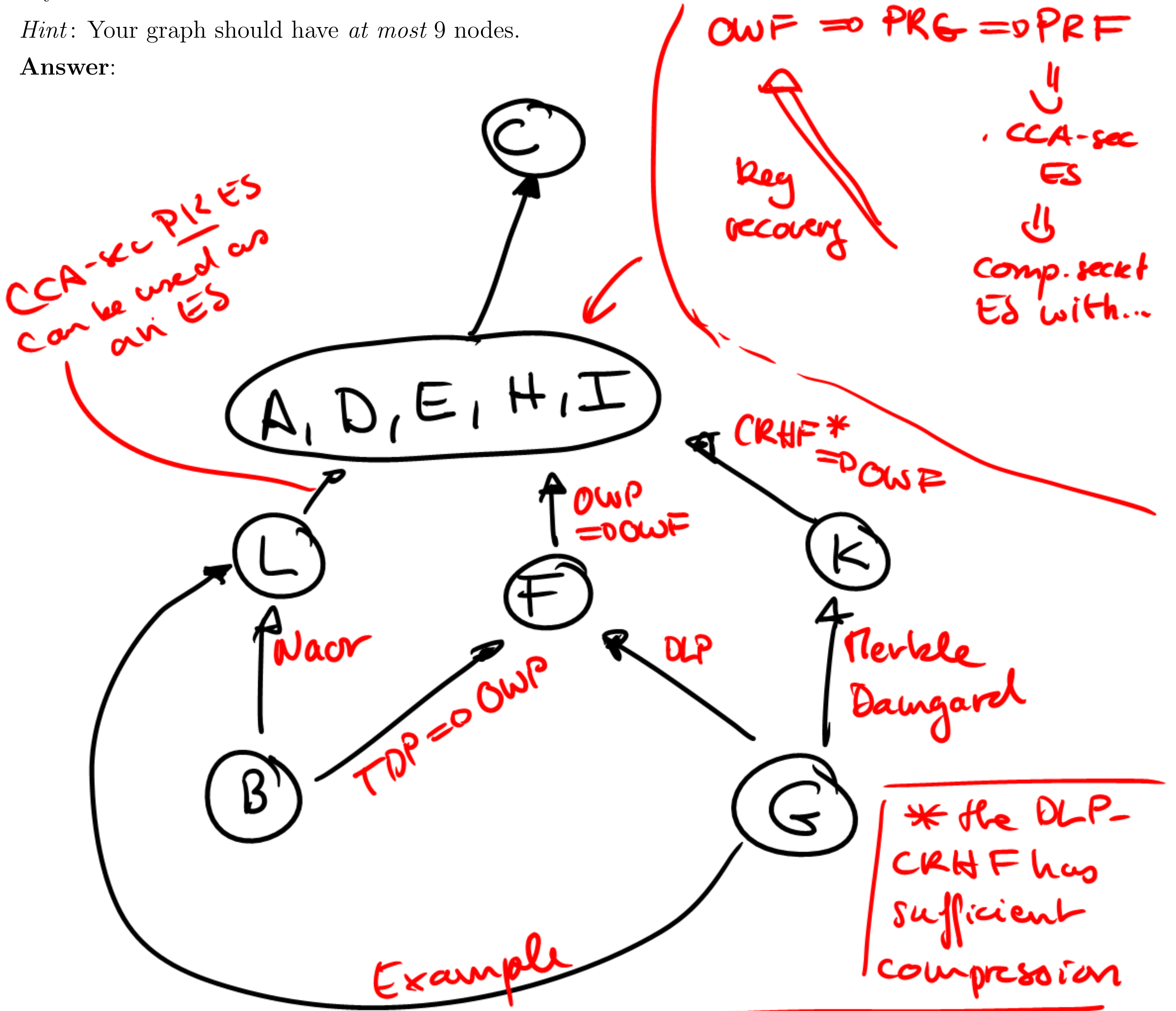
where a **path** from u to v exists *if and only if* the validity of u implies the validity of v **based on the results presented in the lecture**.

Example: $(G) \to (L)$ because of the Cramer-Shoup PKES.

You may merge several nodes into a single node if the validity of any subsumed node implies the validity of any other subsumed node.

Hint: Your graph should have *at most* 9 nodes.

Answer:



RED ≙ additional explanations (not required)

Exercise 2 2P+1P+2P+3P=8P

(a) Let F be a PRF of key and block length n.

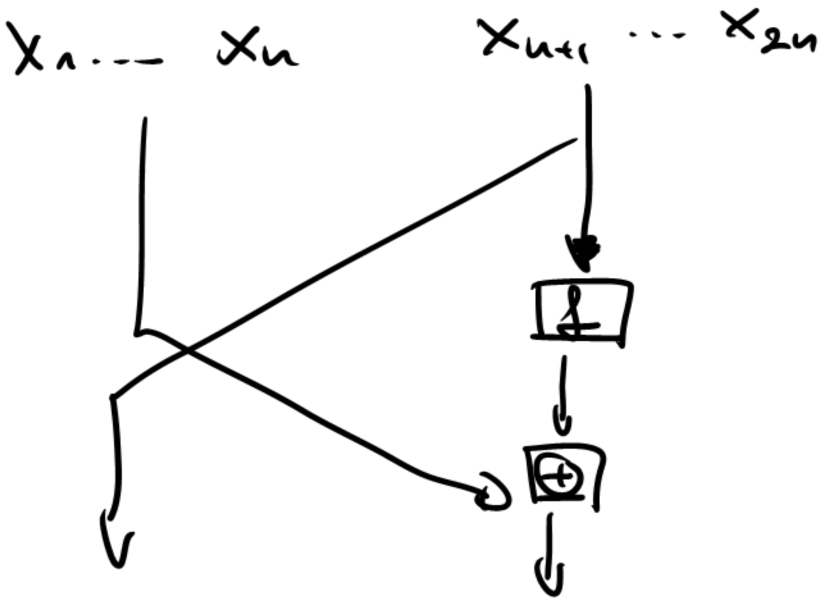
Construct from F a PRP. State all necessary details!

Explicitly state the key and block length of the constructed PRP.

Answer:

Feistel Network FN_f:

$$FN_f(x_1 \dots x_n \, x_{n+1} \dots x_{2n}) := x_{n+1} \dots x_{2n} \, \| \, (x_1 \dots x_n) \oplus f(x_{n+1}, \dots x_{2n})$$



PRP construction given PRF F:

$$P_{k_1\|k_2\|k_3}(\underbrace{x_1 \dots x_{2n}}_{x}) := FN_{F_{k_1}} \circ FN_{F_{k_2}} \circ FN_{F_{k_3}}(x)$$

$x \in \{0,1\}^{2n} \rightsquigarrow$ block length: $2n$

$k = k_1\|k_2\|k_3 \in \{0,1\}^{3n} \rightsquigarrow$ key length: $3n$

(b) Let P be a PRP of key and block length n.

i) Construct from P a PRG of stretch $l(n) = 3n$.

Answer:

$$G(k) := P_k(\lfloor 0 \rceil) \| P_k(\lfloor 1 \rceil) \| P_k(\lfloor 2 \rceil)$$

where $\lfloor \cdot \rceil$ encodes the integers $\mathbb{Z}_{2^n}$ as n-bit strings.

ii) Construct from P a CPA-secure private-key encryption scheme.

Remark: It suffices to define Gen and Enc.

Answer:

Gen: given 1^n, output $k \overset{u}{\in} \{0,1\}^n$

Enc: given $k \in \{0,1\}^n$, $m \in \{0,1\}^*$

1) Pad m to a multiple of n

$\rightsquigarrow m := m\,10\ldots0$

2) Split m in subsequent n-bit blocks:

$m = m^{(1)} \| \ldots \| m^{(\ell)}$

3) Generate $g \overset{u}{\in} \mathbb{Z}_{2^n} \cong \{0,1\}^n$

4) Output $c = g \| c^{(1)} \| \ldots \| c^{(\ell)}$

with $c^{(i)} = m^{(i)} \oplus P_k(\lfloor g+i \rceil)$

(see r CTR or r OFB or r CBC)

(c) Let (Gen_E, Enc, Dec) be a CPA-secure ES and (Gen_M, Mac, Vrf) a secure MAC.

Construct from these a CCA-secure ES (Gen^*, Enc^*, Dec^*).

Explicitly define all three algorithms!

Answer:

Gen: given 1^n, generate $k_E :\stackrel{r}{=} \mathrm{Gen}_E(1^n)$,
and $k_M :\stackrel{r}{=} \mathrm{Gen}_M(1^n)$,
output $k = (k_E, k_M)$

Enc: given $k = (k_E, k_M)$ and $m (\in \mathcal{M}_{Enc})$
1) compute $c :\stackrel{r}{=} \mathrm{Enc}_{k_E}(m)$
2) compute $t :\stackrel{r}{=} \mathrm{Mac}_{k_M}(c)$
3) output (c, t)

Dec: given $k = (k_E, k_M)$ and (c, t).
1) if $\mathrm{vrf}_{k_M}(c, t) = 0$,
output "invalid MAC tag" ($\perp$).
2) else: output $\mathrm{Dec}_{k_E}(c)$

(see Enc-then-Mac)

Exercise 3 **3P+1P+2P=6P**

A friend of yours proposes the following scheme "PWDF" (password-derivation function) to derive passwords for websites from a secret key:

- Let F be a PRF of block and key length n.
- Let k be a secret n-bit key uniformly chosen at random ($k \overset{u}{\in} \{0,1\}^n$).
- Let $u \in \{0,1\}^*$ be the url of the webpage (in some binary encoding).
- Compute an n-bit password of the url u as follows:

  Partition u into subsequent n-bit blocks $u^{(1)}, \ldots, u^{(l)}$ (pad the last block with 0 if necessary).

  Set $t^{(0)} = 0^n$.

  Compute $t^{(i)} := F_k(t^{i-1} \oplus u^{(i)})$ for i from 1 to l.

  Output $\mathsf{PWDF}_k(u) := t^{(l)}$ as password.

This CBC-MAC w/o padding!

Your friend claims that PWDF satisfies the following security definition:

Every PPT-algorithm $\mathcal{A}$ has only a negligible probability w.r.t. n to succeed in the following experiment:

1. Choose $k \overset{u}{\in} \{0,1\}^n$.
2. Run $(u, w) :\overset{r}{=} \mathcal{A}^{\mathsf{PWDF}_k}(1^n)$.

   $\mathcal{A}$ has *oracle access* to PWDF_k in order to simulate that a password might get stolen from a webpage.

▷ $\mathcal{A}$ succeeds if both (i) $\mathsf{PWDF}_k(u) = w$ **and** (ii) $\mathcal{A}$ has not queried the oracle PWDF_k for the image of u.

(a) Show that your friend is wrong by forging a password for the url $0^n || 0^n$.

Answer:

1. $y := \mathsf{PWDF}_k(0^n) = F_k(0^n \oplus 0^n) = F_k(0^n)$

2. $z := \mathsf{PWDF}_k(y) = F_k(0^n \oplus y) = F_k(y)$

$\rightsquigarrow$ Computation of $\mathsf{PWDF}_k(0^n || 0^n)$:

$t^{(0)} = 0^n$

$t^{(1)} = F_k(t^{(0)} \oplus 0^n) = F_k(0^n) = y$

$t^{(2)} = F_k(t^{(1)} \oplus 0^n) = F_k(y) = z$

So z can be obtained without computing $\mathsf{PWDF}_k(0^n || 0^n)$ directly.

(see the prefix attacks on extended PRFs / MACs)

(b) Your friend's security definition has been used for another cryptographic scheme in the lecture. State the name of this scheme.

Answer:

This is exactly the definition of secure MACs (for a particular key generator)

(c) Briefly describe how PWDF has to be *extended* so that it satisfies the security definition of your friend.

Answer:

Fix: Use a padding scheme which prevents the adversary from doing prefix queries.

That is: replace u by

$$\lfloor |u| \rceil \| u$$

where the length $|u|$ of u is encoded using n bits (the block length of F)

Any other way* to prevent prefix-queries on the CBC-constructions is of course also fine, e.g. outer encryption using a second key. (*discussed in the slides)

Exercise 4 **2P+2P+3P=7P**

Recall: Let N be a positive integer. The Carmichael function maps N to $\lambda(N) := \min\{k > 0 \mid \forall x \in \mathbb{Z}_N^* \colon x^k \equiv 1 \pmod{N}\}$. For any $a \in \mathbb{Z}$ let $\exp_{a,N} \colon \mathbb{Z}_N^* \to \mathbb{Z}_N^* \colon x \mapsto x^a \bmod N$.

(a) Consider specifically $N = 7 \cdot 11 \cdot 13 = 1001$.

Determine the *least positive* $d \in \mathbb{Z}$ such that $\exp_{d,1001}$ is the inverse of $\exp_{7,1001}$.

Remark: $\mathsf{gcd}(7, \lambda(1001)) = 1$.

Answer:

$\lambda(7 \cdot 11 \cdot 13) = \operatorname{lcm}(6, 10, 12) = 60$

Extended Euclidean algorithm: gcd(7, 60).

a	b	k
7	60	8
4	7	1
3	4	1
1	3	$\rightsquigarrow \begin{pmatrix}1\\0\end{pmatrix}$

$$\begin{pmatrix}-8 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}-1 & 1\\1 & 0\end{pmatrix}\underbrace{\begin{pmatrix}-1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}}_{\begin{pmatrix}-1\\1\end{pmatrix}}$$

$$\begin{pmatrix}-17\\2\end{pmatrix} \qquad \begin{pmatrix}2\\-1\end{pmatrix} \qquad \begin{pmatrix}-1\\1\end{pmatrix}$$

$$= \begin{pmatrix}-17\\2\end{pmatrix}$$

$\rightsquigarrow 1 = -17 \cdot 7 + 2 \cdot 60$

$\rightsquigarrow d \equiv -17 \equiv \underline{\underline{43}} \ (60)$

(b) State one reason why modern RSA-based PKES use randomized padding.

In addition, state the name of one such padding scheme used in practice today.

Answer:

- Otherwise Enc is deterministic and thus not CPA-secure
- OAEP

(c) Let h be a hash function with output length 256 (in bits), e.g. SHA-256.

Further assume that N is a suitable RSA modulus with $N \in [2^{1024}, 2^{1025}]$.

Finally, let $e, d \in \mathbb{Z}^*_{\lambda(N)}$ with $e \cdot d \equiv 1 \pmod{\lambda(N)}$.

Briefly describe how to compute and verify digital signatures based on the *full-domain-hash* heuristic when (N, e) should be the public verification key, and (N, d) the private signing key.

Solution:

Extension of the range of the hash function:

$$K(m) := h(m \| \langle 0 \rangle) \| \ldots \| h(m \| \langle 4 \rangle)$$

· Counter can also be prepended

• "3" is also fine ; the majority* of $\mathbb{Z}_N$ should be covered. (* up to a negligible fraction)

Signing: $t := (K(m)^d \bmod N)$

Verification:

if $t^e \equiv K(m) \pmod N$

then accept the signature

else reject it.

Exercise 5 **1P+2P+2P+2P=7P**

(a) Is 47 a safe prime?

Answer:

Yes. (as $47 = 2 \cdot 23 + 1$ and 23 is a prime.)

(b) Compute the probability that $x \overset{u}{\in} \mathbb{Z}_{47}^*$ is a generator of $\mathbb{Z}_{47}^*$.

Answer:

$$\frac{\varphi(\varphi(47))}{\varphi(47)} = \frac{\varphi(46)}{46} = \frac{22}{46} = \underline{\underline{\frac{11}{23}}}$$

Recall:

- $\langle \mathbb{Z}_p^*, \cdot, 1 \rangle \cong \langle \mathbb{Z}_{p-1}, +, 0 \rangle$
- $\langle \mathbb{Z}_N, +, 0 \rangle$ has $|\mathbb{Z}_N^*| = \varphi(N)$ many generators.

(c) Is 7 a generator of $\mathbb{Z}_{47}^*$? Prove that your answer is correct.

Answer:

Need to check if $7^d \not\equiv 1 (47)$ for $d \in \{2, 23\}$

Obviously: $7^2 \equiv 49 \equiv 2 \not\equiv 1 (47)$

$$7^{23} \equiv 2^{11} \cdot 7 \equiv 32 \cdot 32 \cdot 2 \cdot 7$$
$$\equiv (-15)^2 \cdot 14$$
$$\equiv 225 \cdot 14$$
$$\equiv -10 \cdot 14$$
$$\equiv -140$$
$$\equiv 1 \quad (47)$$

$7^2 \equiv 2 (47)$

$\leadsto$ 7 is not a generator of $\mathbb{Z}_{47}^*$.

(d) Give a generator of $\mathbb{QR}_{47}$. What is the order of $\mathbb{QR}_{47}$?

Answer:

- 7 generates $\mathbb{QR}_{47}$
- $|\mathbb{QR}_{47}| = 23$

Recall:
- $\left(\frac{7}{47}\right) = (7^{23} \bmod 47) = 1$
  $\leadsto$ so $7 \in \mathbb{QR}_{47}$.
- For a safe prime p: every element in $\mathbb{QR}_p \setminus \{1\}$ is a generator of $\mathbb{QR}_p$.

<u>Exercise 6</u> **2P+2P+2P=6P**

(a) Let $\langle \mathbb{G}, \cdot, 1\rangle$ be a finite cyclic group with generator g.

Denote by $q := |\mathbb{G}|$ the order of $\mathbb{G}$.

Assume $q = d \cdot m$ is a composite and let d be a non-trivial factor of q.

Let $y \in \mathbb{G}$.

Show:

If $k \in \mathbb{N}$ satisfies $g^k = y$ in $\mathbb{G}$, then $(k \bmod d)$ is the unique solution of the following problem:

$$\text{Determine } x \in \mathbb{Z}_d \text{ such that } (g^m)^x = y^m \text{ in } \mathbb{G}.$$

Answer:

- If $g^k = y$ in $\mathbb{G}$

then $(g^k)^m = y^m$ in $\mathbb{G}$

- Obviously: $(g^k)^m = g^{k \cdot m} = (g^m)^k$
- As g^m has order d: $(g^m)^k = (g^m)^{k \bmod d}$

- Assume there is some $x \in \mathbb{Z}_d$ s.t.

$$(g^m)^x = y$$

Then: $(g^m)^x = (g^m)^{k \bmod d}$

i.e: $(g^m)^{x - (k \bmod d)} = 1$

i.e: $x \equiv (k \bmod d) \pmod d$

- As $x, (k \bmod d) \in \mathbb{Z}_d$: $x = (k \bmod d)$.

(b) Given are the prime 89 and the generator 3 of $\langle \mathbb{Z}_{89}^*, \cdot, 1 \rangle$.

Your task is to determine $k \in \mathbb{Z}$ such that $3^k \equiv 86 \pmod{89}$.

Proceed as follows:

i) Using the preceding exercise, first determine k modulo 11.

Answer:

Note: • $|\mathbb{Z}_{89}^*| = \mathbb{Z}_{88}$

As stated in (a):

$(k \bmod 11)$ is the unique solution of:

"Find $x \in \mathbb{Z}_{11}$ s.t. $(3^8)^x \equiv 86^8 \ (89)$"

• $86 \equiv -3 \ (89)$

Need to find $x \in \mathbb{Z}_{11}$ s.t.

$$(3^8)^x \equiv (-3)^8 \equiv (3)^8 \ (89)$$

So: $x = 1$ and $k \equiv 1 \ (11)$.

ii) Someone tells you that $k \equiv 5 \pmod 8$. Determine k.

Answer:

By the CRT:

$$\mathbb{Z}_{88} \cong \mathbb{Z}_8 \times \mathbb{Z}_{11}$$

Inverse isomorphism h^{-1}:

$$1 = \gcd(8, 11) = -4 \cdot 8 + 3 \cdot 11$$

$$\rightsquigarrow h^{-1}: \mathbb{Z}_8 \times \mathbb{Z}_{11} \longrightarrow \mathbb{Z}_{88}$$

$$(u, v) \longmapsto (3 \cdot 11 \cdot u - 4 \cdot 8 \cdot v) \bmod 88$$

$$\rightsquigarrow h^{-1}(5, 0) = (133 \bmod 88)$$

$$= \underline{\underline{45}}$$

$$\rightsquigarrow \underline{3^{45} \equiv 86 \ (89)}$$

Alternative:

$$k = 11 \cdot x + 1$$

$$= 8 \cdot y + 5$$

"Brute force": enumerate $x = 0, \ldots, 7$ until $\frac{11 \cdot x + 1 - 5}{8} \in \mathbb{Z}_8$