

ECS 127 Final — Cryptography — Winter 2019

Instructions: Please write neatly, and in clear, grammatical English. Remember that you may not sit near to a partner or friend. The full text of an academic misconduct warning is below.

Your exam has this cover page and then pages numbered 1 to 7. Please check that your copy is complete.

It has been my pleasure teaching you this term. Relax and don't stress out. You got it.

Name:

Sal Salun

Student ID:

Signature:

Seat, as in D15:

Academic misconduct reminder: Any device that can be powered off must be. You may not sit next to someone you know. In that sentence, "next to" means to your left, right, directly behind, or diagonally behind; and "someone you know" means that they're a friend or someone you've worked with. If you see anything inappropriate during an exam, please report it right away. Please remember my policy about academic conduct, that any incident of academic misconduct will result in getting an "F" in the course.

Blockciphers

1. Name some important differences between the blockciphers **DES** and **AES**, filling in the table with contrasting characteristics of your choice. I'll start you out:

DES	AES
64-bit blocks	128-bit blocks
Feistel network	Substitution-Permutation (SP) network
56-bit keys	128/192/256-bit keys
not well-supported by modern HW	well-supported by modern HW
HW-centric (1970's era)	SW & HW efficient
secret, NSA-directed, corporate process	open-design process/competition

2. Give a precise, quantitative, self-contained statement of the PRP/PRF switching lemma.

Let $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF. Let A be and adv. That asks at most q queries. Then

$$|\text{Adv}_F^{\text{PRP}}(A) - \text{Adv}_F^{\text{PRF}}(A)| \leq \frac{q^2}{2^{n+1}}$$

Let A ask at most q queries. Then

$$|\Pr[\pi \leftarrow \text{Perm}(n) : A^{\pi(\cdot)} \Rightarrow 1] - \Pr[p \leftarrow \text{Func}(n,n) : A^{p(\cdot)} \Rightarrow 1]| \leq \frac{q^2}{2^{n+1}}$$

Message Authentication Codes (MACs)

3. Let $F: \mathcal{K} \times \mathcal{M} \rightarrow \{0,1\}^n$ be a message authentication code (MAC). Formally define the real number $\text{Adv}_F^{\text{mac}}(A)$, the advantage of an adversary attacking F . Make sure to define any specialized terms you need.

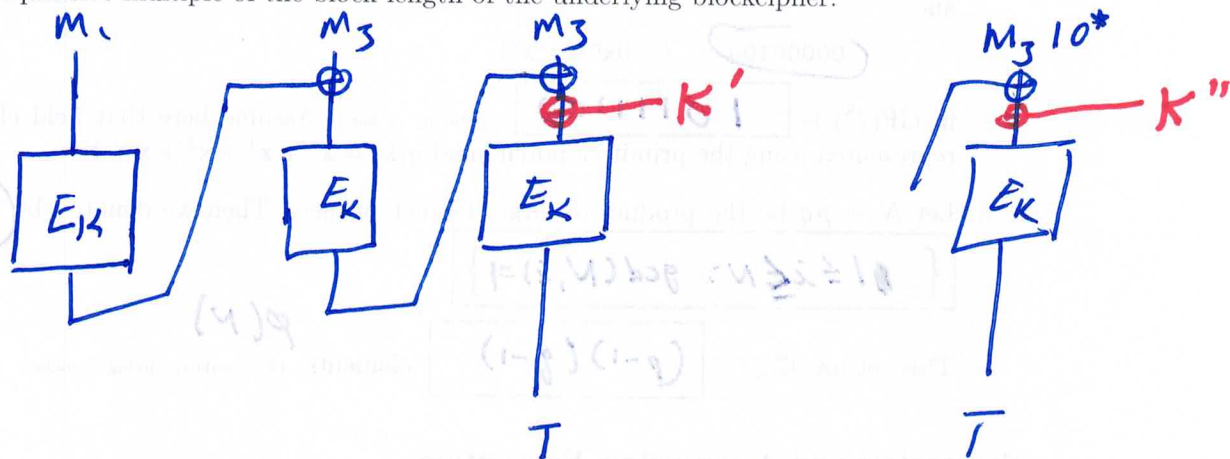
$$\text{Adv}_F^{\text{mac}}(A) = \Pr[K \leftarrow \mathcal{K} : A^{F_K(\cdot)} \text{ Forges}]$$

A outputs (M^*, T^*) where $F_K(M^*) = T^*$ and A never asked its oracle M^* .

4. The raw CBC MAC, shown below, is not secure (as a MAC, across messages that can have varying lengths). Draw in a small modification, discussed in class, so that the resulting

pagebreak

construction is secure across messages of varying lengths. Assume here that all messages are a positive multiple of the block length of the underlying blockcipher.



Digital Signatures

5. Diffie and Hellman wanted to make a **digital signature** from a **trapdoor permutation**.

A trapdoor permutation generator $(-f, -g) \leftarrow \mathcal{F}(k)$ would be used to produce a description $-f$ of a permutation f , and a description $-g$ of its inverse g . The function f would be one-way: it would be computationally infeasible to find $g(y) = f^{-1}(y)$ for a uniformly random y . Now for our digital-signature scheme, the **public key** would be $-f$

and the **secret key** would be $-g$. The signer would sign a message m in the

domain of f by transmitting along with m a signature $\sigma = g(m)$. To verify

a signature σ for m , the verifier checks if $f(\sigma) = m$.

In class we explained that the method above is not (write "is" or "is not") a secure way to sign messages when \mathcal{F} is, say, the RSA trapdoor permutation.

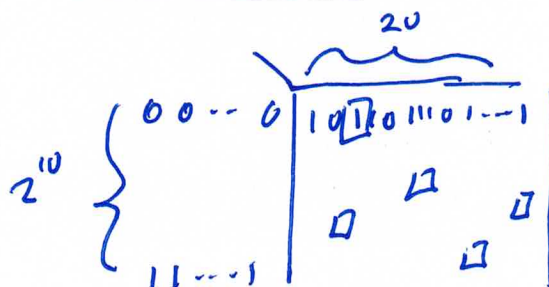
Crypto Math

6. How many **functions** are there from 10 bits to 20 bits?

$$2^{20 \cdot 2^{10}}$$

7. The product of bytes

$$20 \cdot 2^{10}$$



$$\underline{00101111} \quad (= 0x2F = x^5 + x^3 + x^2 + x + 1)$$

and

$$\underline{00000100} \quad (= 0x04 = x^2)$$

in $GF(2^8)$ is $\boxed{10111100}$. (Binary or hex.) Assume here that field elements are represented using the primitive polynomial $g(x) = x^8 + x^4 + x^3 + x + 1$.

8. Let $N = pq$ be the product of large distinct primes. Then we denote by \mathbb{Z}_N^* the set

$$\{1 \leq i \leq N : \gcd(N, i) = 1\}$$

This set has $|\mathbb{Z}_N^*| = \boxed{(p-1)(q-1)}$ elements. (A formula specifying a number)

$$\phi(N)$$

Symmetric and Asymmetric Encryption

9. The encryption algorithm in a scheme for AEAD (authenticated encryption scheme with associated data) takes in four inputs: a key K , a nonce N , associated data A , and a plaintext M . It produces, deterministically, a ciphertext $C = \mathcal{E}(K, N, A, M)$.

Explain the role of the **nonce** N :

The nonce is a value that the user supplies and must not repeat over the course of a session. It ensures that repeated (A, M) pairs aren't visible to the adversary. It's an alternative to making the scheme probabilistic.







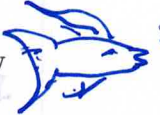






Explain the role of the associated data A :

stuff that is authenticated but not encrypted (=not privacy protected). Eg, headers.

10. What does it mean if we say that an encryption scheme is **nonmalleable**? Don't use the word *malleable* in your description.

It means you can't change a ciphertext C into a ciphertext C' , $C' \neq C$, where the underlying plaintext M' for C' is meaningfully related to the underlying plaintext M for C .

11. Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a **public-key** encryption scheme. Can it be **ind-secure** with each of the following characteristics? Darken Y for yes (it **might** be ind-secure); or N for no (it **can't** be ind-secure). Where strings are written in **text**, you may regard them as ASCII-encoded binary strings; each character encoded in 8-bits.

- N   Y Ciphertexts that encrypt Hello and there are easily distinguished.
- N   Y Ciphertexts that encrypt Hello and mom are easily distinguished.
- N   Y The ciphertext for Hello is always blue fish wrestle endlessly 
- N   Y Every ciphertext begins with blue fish wrestle endlessly
- N   Y Every ciphertext begins with the public key pk that was used to make it.
- N   Y Encrypting Hello takes 2 msecs, while encrypting there take 4 msecs.

Hashing

12. Informally describe what it means for a cryptographic hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$ to be **collision resistant**. (Also called "collision intractable.") Don't use the word *collision* in your answer.

It means nobody knows ~~a collision~~ for it.
~~There~~ M and M' , $M \neq M'$, s.t.
 $H(M) = H(M')$

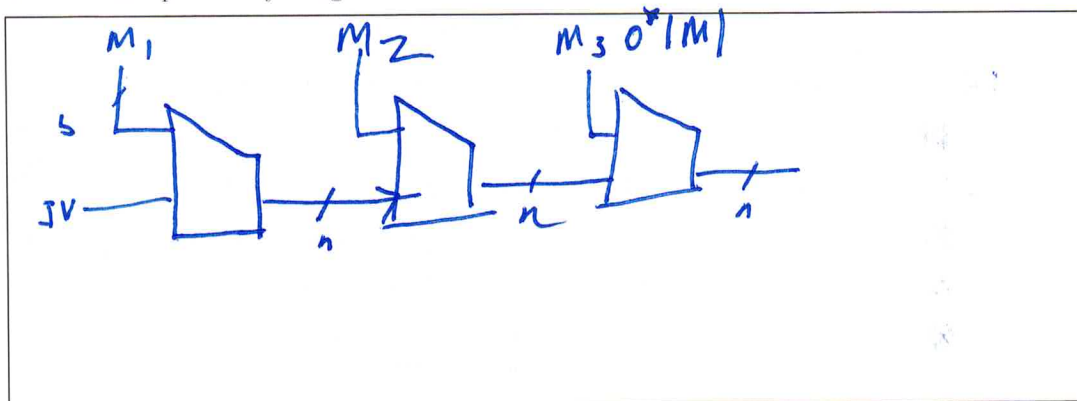
13. Describe some **foundational concern**—a possible paradox—associated to defining collision resistance.

There are lots of collision in H
 but ~~there~~ there aren't any
 (to be found)

$A \xrightarrow{H} H(A)$ 

* in/sec - -

14. Draw a picture of the Merkle-Damgård construction, which turns a compression function $h: \{0,1\}^{b+n} \rightarrow \{0,1\}^n$ into a cryptographic hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$. You needn't prove anything.



Provable Security

15. Let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a blockcipher and let $G: \{0,1\}^k \rightarrow \{0,1\}^\infty$ be a PRG (pseudorandom generator) defined from E by $G(K) = R_1 R_2 R_3 \dots$ where $R_1 = E_K(0)$ and $R_{i+1} = E_K(R_i)$ for all $i \geq 1$. Suppose you wish to prove that

If E is a secure blockcipher then G is a secure PRG.

To prove this statement, you will need to give a **reduction**. For the reduction, you are given an adversary A that

attacks the PRG G

(A does what?)

You will use A to construct an adversary B that

attacks the blockcipher E

(B does what?)

You will need to prove that

$\text{Adv}_E^{\text{pp}}(B)$ is large if $\text{Adv}_G^{\text{prg}}(A)$ is large

(A and B are related how?)

Other

16. Describe some use that can be made of a **garbled circuit**.

17. In a homework problem, we applied Shamir secret sharing byte-wise to a long message $M = M_1 \cdots M_m$, $M_i \in \{0,1\}^8$. In what way is that approach better than applying Shamir's scheme directly to M ?

More efficient

18. What is meant if I say that a scheme is secure in the **random-oracle model** (ROM)? Answer in 2–4 clear and grammatical English sentences.

- You provide everyone and every scheme a random function $H \leftarrow \mathcal{H}$.
- Prove your scheme secure in ROM.
- Instantiate H with a real-world hash function

True or False

19. For each of the following claims, darken T for true or F for false. Wrong answers will be penalized, but you should still guess. This problem will count more than other ones.

- (a) F ☒ T ☐ $2^{200} \bmod 11 = 2$
- (b) F ☒ T ☐ In the context of symmetric encryption, ind-security (indistinguishability from the encryption of zero bits) is equivalent to ind\$-security (indistinguishability from random bits).
- (c) F ☒ T ☐ Perfect privacy, discussed near the beginning of our class, is the strongest notion of privacy we considered.
- (d) F ☒ T ☐ If AES is a PRP-secure blockcipher, then CBC encryption with AES and a zero-IV will achieve good ind-security.
- (e) F ☒ T ☐ If E is an ideal PRP (denoted P in one proof we did in class), then CTR encryption with it will achieve perfect privacy.
- 5 (f) F ☒ T ☐ If its key space is larger than its message space, an encryption scheme will achieve perfect privacy.
- (g) F ☒ T ☐ ChaCha20 is a provably secure blockcipher: we know that reasonable adversaries have small prp-advantage in attacking it.
- (h) F ☒ T ☐ Public-key encryption schemes can be secure, in the sense we defined, despite being stateless and deterministic.
- (i) F ☐ T ☒ Digital signature schemes can be secure, in the sense we defined, despite being stateless and deterministic.
- (j) F ☒ T ☐ An AEAD scheme can be secure, in the sense we defined, even if it is length-preserving: $|\mathcal{E}_K^{N,A}(M)| = |M|$.
- (k) F ☐ T ☒ It is possible, we believe, to construct a secure digital signature scheme from a cryptographic hash function such as SHA-256.
- (l) F ☒ T ☐ It is possible, we believe, to construct a secure public-key encryption scheme from a cryptographic hash function such as SHA-256.
- (m) F ☐ T ☒ Asymptotic security definitions require schemes to employ a number-valued security parameter.
- (n) F ☒ T ☐ In his essay *The Moral Character of Cryptographic Work*, Prof. Rogaway says that, in the end, it is not a researcher's role to try to figure out the social costs or benefits of their work, because that is the role of policy makers and the law.
- (o) F ☐ T ☒ The essay sometimes wandered far from cryptography, for example, touching on nuclear weapons, the Nuremberg trials, and the environmental movement.