Final Review Sheet
ENEE 457
Fall 2019

Symmetric Key Cryptography:

Give an example of a symmetric key cryptographic scheme covered in class that achieves privacy and not integrity. Describe the scheme and show an explicit attack against integrity.

Can a CPA-secure symmetric key encryption scheme have a deterministic "Encrypt" algorithm? Why or why not? Can a seucre message authentication code (MAC) have a deterministic Mac algorithm? Why or why not?

Public Key Cryptography:

Describe in detail an attack on Textbook RSA signatures that has the following properties: (1) The attack allows the attacker to sign *any message* of its choice. (2) The attacker makes only a single query to the signing oracle.

Consider the subgroup of Z_{23}^* consisting of quadratic residues modulo 23. This group consists of the following elements: {1; 2; 3; 4; 6; 8; 9; 12; 13; 16; 18}. We choose g = 2 to be the generator of the subgroup.
Consider two parties running Diffie-Hellman key exchange. One party chooses x = 5, the other party chooses y = 3.
Show the messages sent between the two parties and the final shared key reconstructed by both. Do the computations by hand and show your work.

Hint: To speed up your computations, use the fact that $3^3 = 4 \, mod \, 23$, $8^4 = 2 \, mod \, 23$, $4^{-1} = 6 \, mod \, 23$.

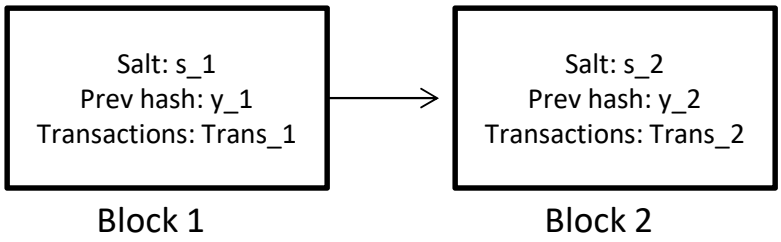
Applications:
How does a certificate authority (CA) use digital signature schemes to generate certificates?

How are public key cryptography and symmetric key cryptography combined in order to communicate securely over the internet?

Give two examples of ways cryptographic schemes can be misused in practice.

Bitcoin

Assume the current Blockchain looks like the following and that the current difficulty level is n.



In order to successfully mine the next block (Block 2), a miner needs to find a salt s_3 such that h(s_3, x) = y_3, for x,y_3 of a specific form. What is x in the above example? What is the form of y_3?

Differential Privacy

Show that mechanism M defined below is not differentially private, using the definition of differential privacy and the databases D and D' defined below.

M randomly chooses a set of 3 records and returns the number of UMD students in the randomly chosen set.

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Daniel	1
Edgar	0

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Edgar	0

Dining Cryptographers/MixNets

Assume there are three dining cryptographers, P_1, P_2, P_3. Each wants to broadcast a message m_1, m_2, m_3, but at most one party can successfully broadcast a message in each round. Assume the parties have agreed to run the protocol for several rounds. At the beginning of each round each party flips a coin. If it is heads, the party broadcasts a message. If it is tails the party does not broadcast its message. Explain what each party should broadcast in each round. On average, how many times will the parties need to run the protocol for each message to be broadcast? How will the parties know when all three messages are broadcast.

Password Hashing

Briefly explain what a Rainbow Table is.

In class we saw that adding a “salt" to the hash can prevent attacks via Rainbow Tables. Is this countermeasure still effective if a 256-bit “salt" is chosen, but the same “salt" value is used for each entry in the password table? Explain your answer.

Briefly list some properties of a good password hash and explain why they are desirable for a password hash, but may not be desirable for other settings.

Consider the following graph (Figure 1) showing the memory usage of a hash function H over time when evaluated on a single input x. Let H' be a hash function that on input $(x_1||x_2)$, outputs $H(x_1)||H(x_2)$. How can we minimize the space-time complexity of the computation of H'? (Recall that the space-time complexity is the maximum amount of space used in any time step multiplied by the number of time steps.) Draw a graph on the back of the page showing the memory usage of H' over time.

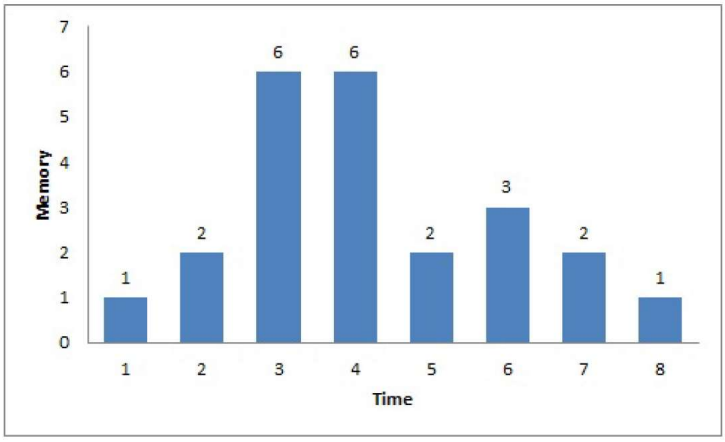


Figure 1: Memory usage of H over time

Network Security

What is TCP/IP?

What is Packet Sniffing/Spoofing and what tools can be used to perform these actions?

What is the TCP 3-way handshake?

Name 3 TCP Header “code bits” (also called flags) and what they do.

What is the significance of the sequence number and acknowledgement number in a TCP header?

What is a SYN Flooding attack?

What is a TCP RST attack?

What is a session hijacking attack?

What is a reverse shell?

Side-Channel Attacks

What is a side-channel attack?

What is a cache timing channel?

What is the Flush+Reload Technique?

What is exception handling?

What is out-of-order execution?

How can one check that out-of-order execution indeed occurred using the Flush+Reload technique?

How can one learn secret information by leveraging out-of-order execution and the Flush+Reload technique (as in the Meltdown attack)?

Adversarial machine learning

Inputs in the training set are 0/1 vectors of dimension n.

Assume the target function is $x_1 \vee x_2 \vee x_3 \ldots \vee x_n$

Examples occurring in the training set all satisfy $x_2 \neq x_3$.

Give an example of a model that might be output by a machine learning algorithm that would correctly classify all the examples in the training set.

Give an example of an adversarial input that is misclassified by your model given above.