Jeopardy:

Please sit in groups of up to 6!

Crypto 1	Crypto 2	Web Security	Authenti-cation	Grab Bag
100 Points	100 Points	100 Points	100 Points	100 Points
200 Points	200 Points	200 Points	200 Points	200 Points
300 Points	300 Points	300 Points	300 Points	300 Points
400 Points	400 Points	400 Points	400 Points	400 Points
500 Points	500 Points	500 Points	500 Points	500 Points

Final Jeopardy:

How do solutions like Convergence help with the problem of trusting Certificate Authorities?

Final Jeopardy Answer:

By decentralizing trust: they compare certificates seen by different nodes, assuming that not everyone is currently subject to a MiTM attack.

This cryptographic construction is used to protect message integrity.

What is a message authentication code (MAC)?

The difficulty of this mathematical problem is why RSA is assumed to be secure.

What is modular inversion (or, the factoring problem)?

This is the definition of the one-wayness property for hash functions.

What is "Given y, it should be hard to find any x such that h(x) = y"?

This block cipher mode is insecure because the same plaintext is always encrypted to the same ciphertext.

What is Electronic Codebook (ECB) mode?

This construction is used to build invertible functions out of non-invertible functions.

What is a Feistel network?

This cryptographic construction should be used to protect both integrity and secrecy.

What is Encrypt-then-MAC?

The difficulty of this mathematical problem is why Diffie-Hellman is assumed to be secure.

What is the discrete log problem?

This is the definition for the collision resistance property for hash functions.

What is "It should be hard to find distinct x and x' such that $h(x) = h(x')$"?

Repeating this in an implementation of CTR or CBC mode will make the block cipher insecure.

What is the counter value (CTR mode) or the IV value (CBC mode)?

For this reason, the repeated squaring method of optimizing exponentiation is insecure.

What is information leaked from timing differences?

This type of attack is possible when a website echoes back user input without sanitizing.

What is cross-site scripting (XSS)?

This type of attack tricks a user into clicking on a sensitive button, using visual or timing tricks.

What is clickjacking?

In this type of attack, the user's browser is pointed to a sensitive URL, taking advantage of automatic cookie sending.

What is cross-site request forgery (XSRF)?

This policy, enforced by browsers, prevents iframes from accessing the parent page, and vice versa.

What is the same-origin policy?

This technique is used by web trackers to repopulate identifiers when users clear their browser cookies.

What is respawning, or zombie cookies?

This technique is used to greatly increase the cost of dictionary attacks on password lists.

What is salting or peppering?

This is the term for an authentication scheme that involves something you know and something you have.

What is two-factor authentication?

This is the term for the rate at which a biometric system incorrectly rejects a user.

What is insult rate?

This is the term for the rate at which a biometric system incorrectly accepts a user.

What is fraud rate?

This is the formula for calculating the number of bits of entropy in a password.

What is $\log_2$(# of possible passwords)?

This is a common cause of buffer overflow vulnerabilities.

What is no bounds checking on string copying?

What is the name of the most popular system used by individuals who want anonymity online?

What is Tor?

This is Kerckhoff's Principle.

What is "The security of a crypographic object should depend only on the secrecy of the key, not of the algorithm"?

This is a fundamental difference between isolation in Android versus in traditional desktop OSes.

What is “apps are isolated, rather than users”?

This technique avoids non-executable stack restrictions by patching together sequences of existing instructions.

What is return-oriented programming?