12 Angry Squares	Saving Private Enc**Ry**pti**an**	It’s not rocket signs!	To share, or not to share, that’s the key	Prove it!
100	**100**	**100**	**100**	**100**
200	**200**	**200**	**200**	**200**
300	**300**	**300**	**300**	**300**
400	**400**	**400**	**400**	**400**
500	**500**	**500**	**500**	**500**

12 Angry Squares

100

Be this or be a square (in $\mathbb{Z}_p^*$) :)

Question
Answer
Done!
Home

12 Angry Squares

100

What is a generator?

Question
Answer
Done!
Home

12 Angry Squares

200

This sgroup consists of (or this notation represents) the set of all numbers from 0 to N-1 for positive integer N

Question

Answer

Done!

Home

12 Angry Squares

200

What is $\mathbb{Z}_N$?

Question

Answer

Done!

Home

12 Angry Squares

300

This integer is present in $\mathbb{Z}_p$ but not $\mathbb{Z}_p^*$ for prime p.

12 Angry Squares

300

What is 0?

$\mathbb{Z}_p = \{$0,1,..p-1$\}$

$\mathbb{Z}_p^* = \{$1,..p-1$\}$

Question

Answer

Done!

Home

12 Angry Squares

400

$\mathbb{Z}_N^*$ is cyclic if N is this type of number

12 Angry Squares | 400

What is a prime?

Question
Answer
Done!
Home

12 Angry Squares

500

For a safe prime p, $g \in \mathbb{Z}_p^*$ is a generator if and only if these two conditions hold true

Question
Answer

Done!
Home

12 Angry Squares

500

What are $g^2 \pmod{p} \equiv 1$ and $g^q \pmod{p} \equiv 1$

Question
Answer

Done!
Home

Saving Private encRYptiAN

100

This is an attack against an RSA encryption scheme that uses a low public exponent.

Question
Answer

Done!
Home

Saving Private encRYptiAN

100

What is Hastad's Broadcast Attack?

Question Answer

Done! Home

Saving Private encRYptiAN

200

This type of encryption scheme allows the sender to use an arbitrary string like an email address or URL as the receiver's public key while the receiver can obtain the secret key from a central authority.

Saving Private encRYptiAN

200

What is identity based encryption?

Question
Answer
Done!
Home

Saving Private encRYptiAN

300

This recently discovered theoretical type of encryption scheme allows users to compute any arbitrary function on encrypted data.

Question
Answer

Done!
Home

Saving Private encRYptiAN

300

What is fully homomorphic encryption?

Question
Answer

Done!
Home

Saving Private encRYptiAN

400

The attack against this scheme as used in the PKCS1 standard showed that the notion of IND-CPA security is not strong enough to capture all practical attacks.

Question Answer

Done! Home

Saving Private encRYptiAN

400

What is plain RSA? (the attack was Bleinchenbacher's attack)

Saving Private encRYptiAN

500

When this transform is applied to a message before performing RSA encryption, the resulting encryption scheme becomes IND-CCA secure under the RO model, assuming RSA is hard.

Question
Answer

Done!
Home

Saving Private encRYptiAN

500

What is OAEP? (What is Optimal Asymmetric Encryption Padding?)

It's not rocket signs!

100

This variation of a group signature scheme does not have a group manager.

Question
Answer

Done!
Home

It’s not rocket signs!

100

What is ring signature?

Question Answer

Done! Home

It’s not rocket signs!

200

This signature scheme is a randomized variant of FDH-RSA that offers better security guarantees and is part of the latest PKCS standard.

Question
Answer

Done!
Home

It's not rocket signs!

200

What is PSS? (Probabilistic Signature Scheme)

Question

Answer

Done!

Home

It's not rocket signs!

300

This is the **property** of a signature scheme where the signer has no information about the message they are signing.

Question Answer

Done! Home

It's not rocket signs!

300

What is blindness or anonymity?

Question

Answer

Done!

Home

It's not rocket signs!

400

This DL based signature scheme is as efficient as ECDSA when implemented in a 160b elliptic curve group and is proven secure in the Random oracle model under the DL assumption.

(Hint: It has looser security guarantees than other DL based signature schemes)

Question
Answer

Done!
Home

It’s not rocket signs!

400

What is Schnorr signature?

It's not rocket signs!

500

This property is an advantage of public key signature schemes over MACs and refers to the fact that the verifier cannot impersonate the sender.

Question
Answer

Done!
Home

It's not rocket signs!

500

What is non-repudiation?

Question

Answer

Done!

Home

Key Sharing | 100

This trusted third party acts as a “starting point” for verifying key authenticity and is the most common basis for public key infrastructure.

Question
Answer
Done!
Home

Key Sharing

100

What is Certificate Authority?

Question
Answer

Done!
Home

Key Sharing

200

This is one of the biggest problems for widespread deployment of PKI and public key cryptography
(Hint: This problem relates to keeping track of bad certificates on a security breach.)

Question
Answer

Done!
Home

Key Sharing

200

What is Revocation?

Question

Answer

Done!

Home

Key Sharing

300

This practice of adding a random number input to the hash helps protect against mass cracking of compromised passwords but is still ineffective at protecting a single user's password.

Question

Answer

Done!

Home

What is salting?

Question

Answer

Done!

Home

Key Sharing

400

Known public keys, previously shared public keys (through some interaction) or a key shared with a trusted third party server are examples of this type of information advantage.

Question
Answer

Done!
Home

Key Sharing | 400

What is long term key?

Question
Answer

Done!
Home

Key Sharing

500

This mathematical technique is used to recover the secret k from t portions of the secret in Shamir's secret sharing scheme.

Question
Answer

Done!
Home

Key Sharing

500

What is Lagrange Interpolation?

Question
Answer
Done!
Home

Prove it! | 100

This technique is used to prove schemes are secure rather than insecure.

Question
Answer

Done!
Home

Prove it!

100

What is contraposition? (or proof by reduction)

Question
Answer

Done!
Home

Prove it! | 200

This encryption scheme can be proven to be NOT IND-CPA secure in $\mathbb{Z}_p^*$ based on the ability to distinguish squares from non-squares in $\mathbb{Z}_p^*$

Question
Answer

Done!
Home

What is ElGamal encryption scheme?

Prove it!

300

If CDH is proven to be easy in a group G, then this problem is easy in G but this problem is not. (order of responses is important here)

Question
Answer

Done!
Home

Prove it! 300

What are DDH and DL respectively?

CDH is easy $\implies$ DDH is easy.

CDH is easy $\not\Rightarrow$ DL is easy (but DL is hard $\implies$ CDH is hard)

Question
Answer

Done!
Home

Prove it! | 400

This security definition presents the adversary with n (pk, sk) pairs and n encryption oracles for a single challenge bit b. The adversary is allowed to query the oracles in any order, including adaptively, and the advantage of the adversary is based on their success in distinguishing left-vs-right experiments.

Question
Answer

Done!
Home

Prove it!

400

What is multi-user IND-CPA security?

Question

Answer

Done!

Home

Prove it! | 500

In this experiment, the adversary is given public key (N, e), and a y such that $y = g^x$ for an x chosen randomly from $\mathbb{Z}_N^*$. The adversary is said to be successful if they output a number $x' = x$ and their advantage is defined as the probability of succeeding.

Question | Done!

Answer | Home

Prove it! 500

What is ow-kea? (Onewayness under known exponent attack)

Question Answer

Done! Home