Here are ten math/cs toss-ups I wrote for a vanity pack, except basically all the math questions are algebra and all the cs questions are cryptography.

1. The Fujisaki–Okamoto transform is used to construct algorithms for performing this process. One such algorithm, which takes its name from the crystals used to power lightsabers, is Kyber. Kyber contains encapsulation and decapsulation steps, typical of all KEMs, a type of algorithm used to perform this process. The result of another method of carrying out this process is a primitive root raised to two secret exponents, each chosen by one of the participants. That result is then typically used for encryption using a symmetric key algorithm. Diffie and Helman name one method for carrying out this process. For 10 points, name this process by which a shared cryptographic secret is established.
ANSWER: **key exchange** (accept answers describing sharing a key, or shared secret until mention; prompt on **encryption**)

2. Schur's Lemma determines the nature of maps between two of these structures, based on whether the two structures are isomorphic. Schur's Lemma is a fundamental result of representation theory, which studies homomorphisms between groups and these structures. The analogue of this structure over rings is called a module. The set of linear functional from one of these structures to its base field is called the dual space and is once again one of these structures. Inner products can be defined on these structures and are a generalization of the dot product. For 10 points, name these sets of objects that have a magnitude and direction and are studied in linear algebra.
ANSWER: **vector space** (accept **representation**s until mention)

3. Lamport signatures are usually constructed using these functions. Many such signatures can be handled by a tree which stores the output of these functions in its non-leaf nodes, the Merkle tree. A version of this function released in 2015 has a sponge based construction, which solves the vulnerability previous versions had to length extension attacks. These vulnerabilities arose from their Merkle-Damgård construction. To be cryptographically secure, these functions must be pre-image resistant, second pre-image resistant, and collision resistant, with one such example being SHA-3. For 10 points, name these one-way functions, which are used in namesake tables to speed up look-up time.
ANSWER: **hash** function

4. Q adjoin the third root of 2 does not have this property over Q, but it does over Q adjoin a primitive cube root of unity. For a finite Galois extension, the Galois correspondence gives bijection between Galois subextensions and subgroups of the Galois group with this property. This term describes a field extension in which all polynomials irreducible in the base field either stay irreducible, or split fully into linear factors. A_5 has no proper subgroups with a property described by this word, meaning it is simple, because it has no proper subgroups that are preserved by conjugation. The Gram-Schmidt process outputs a basis which is orthogonal and has this property. For 10 points, identify this word which describes vectors perpendicular to a surface at a given point.
ANSWER: **normal**

5. To achieve this property, the Fujisaki–Okamoto transform vitally derandomizes a public key encryption scheme, allowing a re-encryption check to be computed. Naive El Gamal does not possess this property while hashed El Gamal does, due to the malleability of the unhashed version. One variant of this property

allows adaptive queries until a certain point, and is known as the lunchtime attack. This property can be proven using a game where an adversary has access to both a decryption oracle and an encryption oracle, and must distinguish whether a challenge is randomly generated. For 10 points, name this cryptographic property that is stronger than chosen-plaintext-attack, or CPA, security.
ANSWER: IND-**CCA** security (accept answer describing indistinguishability or security under **chosen-ciphertext** attacks)

6. The relative form of this quantity is calculated as the sum over x, of p of x, times logarithm of p of x over q of x. That relative form measures how much a model distribution Q differs from a true distribution P, and is known as KL divergence. Kraft's inequality can be used to prove that this quantity provides a theoretical lower bound for expected length of any encoding of a message. This quantity represents how much information is communicated by a given message. It is calculated as the sum over x, of p of x, times the logarithm of 1 over p of x. For 10 points, what information theoretic quantity named after Claude Shannon is analogous to one in statistical mechanics that measures the disorder in a system.
ANSWER: information **entropy** (or Shannon **entropy**; accept **KL divergence** until read; accept **I-divergence**)

7. Acting on the permutation representation of a group, this object is the only one to have a non-zero character, and the character of this object is always the dimension of a representation. Negative one is an example of this object in the projective special linear group, and similarly so is any pair of two disjoint two cycles in S_4 mod the Klein Four Group. Any element acts as this object for its own coset, and the orbit of this object is the entire group. If the kernel linear transformation consists only of this object, then that transformation is injective. For 10 points, name this element which leaves all other unchanged under the group operation, denoted 1 in multiplicative notation.
ANSWER: **identity** element (prompt on **1** before mention; prompt on **0**; prompt on **e**)

8. The number of these objects is the number of irreducible representations of a group. When calculating orbit size with Burnside's lemma, the number of fixed points can be computed once for each of these objects, with the results combined in a weighted sum, since the number of fixed points is the same for all elements in a common one of these objects. In Sn, these objects are determined entirely by cycle shape. Normal subgroups must be the unions of these objects. The value of the trace is the same on all elements in a common one of these objects, which for matrices corresponds to similarity. For 10 points, name this object, which, for an element h, is defined as all elements which can be written as $g\ h\ g^{-1}$, for some g in G.
ANSWER: **conjugacy class**

9. One case of this task can be performed by solving a quadratic polynomial, if phi of n is known, and performing this task for n is computationally equivalent to finding square roots modulo n. One algorithm for this task relies on the birthday paradox, and generates a sequence by iteratively applying a polynomial until a value is repeated, which causes a cycle that is detected by Floyd's algorithm. Pollard's Rho algorithm can be used to solve this problem classically. It's not the discrete logarithm, but since this problem can be reduced to a period finding problem, it can be solved on a quantum computer via Shor's algorithm, which threatens the security of RSA. For 10 points, name this task which involves decomposing an integer into prime numbers.

ANSWER: integer **factorization** (or prime **factorization** or **factoring**; I guess prompt on **finding roots** of a polynomial)

10. A four-cycle has this many fixed points when acting on the vertices of a cube, and a three-cycle has this many fixed points when acting on the faces of a cube. If a non-abelian group has this many normal subgroups, it cannot be solvable. In *contrast* to Cauchy's theorem, this is how many elements of a certain order you are *guaranteed*, if that order divides the non-prime cardinality of a group. By Lagrange's theorem, this is the number of even ordered elements in a group of odd order. A_5 has this many nontrivial proper normal subgroups. Definitions of the natural numbers sometimes differ on whether they include this number. For 10 points, in additive notation, which number denotes the identity?
ANSWER: **zero** (accept **none**)