Grading comments: The exam was graded out of 120 points (10 points per problem, with problem 13 contributing an EC point or two).

1. Consider the problem of achieving privacy in the public-key setting (the problem solved by public-key encryption problem). If Alice wants to send a private message $M$ to Bob, then Bob generates a public key $P_k$ and a corresponding secret key $S_k$. Alice computes a ciphertext $C$ for plaintext $M$ as a function of $M$ and $P_k$.

2. In the dating problem, Alice holds a bit $a \in \{0, 1\}$ and Bob holds a bit $b \in \{0, 1\}$. We intend that $a = 1$ when Alice wants to go on a date with Bob, and $b = 1$ when Bob wants to go on a date with Alice. Alice and Bob want to compute $a \land b$ in such a way that each party learns only this. We don’t care if Alice learns $b$ when $a = 1$, or if Bob learns $a$ when $b = 1$, because this is inherently revealed by knowing ones input bit and the conjunct of the inputs.

3. In a single sentence, describe Kerckhoff’s principle: A cryptosystem should remain secure if all aspects of it, except the secret key, are made know to the adversary.

4. Alice uses a substitution cipher with an alphabet $\Sigma$ that consists of the 95 printable ASCII characters. How many possible keys are there? $95!$

5. Consider Diaconis’s algorithm for breaking a substitution cipher. It assumes we have values $M[x, y]$ describing the likelihood of each bigram $(x, y)$, where $x, y \in \Sigma$ (and so $\sum_{x, y \in \Sigma} M[x, y] = 1$). The algorithm defines the plausibility of a candidate plaintext $M = x_1 \cdots x_m \in \Sigma^m$ as the number $\text{Pl}(M) = \prod_{i=1}^{m-1} M[x_i, x_{i+1}]$.

6. Compute the following number: $\Pr[X \leftarrow \{0, 1\}^{128}; Y \leftarrow \{0, 1\}^{128} : X = Y] = 2^{-128}$.

7. In a picture or in English text, describe some high-level aspect about the algorithm A5/1.

8. We described a (classical) PRG (pseudorandom generator) as a map $G : \{0, 1\}^n \rightarrow \{0, 1\}^N$ with $n < N$. We then measured the efficacy of an adversary $A$ attacking such a PRG $G$ with a real number $\text{Adv}_G(A)$, which Prof. Rogaway defined as

$$\text{Adv}_G(A) = \Pr[K \leftarrow \{0, 1\}^n : A(G(K)) \rightarrow 1] - \Pr[Y \leftarrow \{0, 1\}^N : A(Y) \rightarrow 1]$$

where

--- (nothing needed if written as clearly as the above)

9. How many 10-character passwords are there of the form: nine of the characters are lower-case English letters, while one of the characters is an upper-case English letter. $10 \cdot 26^{10}$.

10. False. There is a finite field, GF(100), on 100 points.

   Finite fields must have a number of elements that’s a power of a prime.
11. Draw a picture showing two rounds of a Feistel network (the construction used in DES). Label the input block $M = M_1M_2$ with $M_1$ and $M_2$, where $|M_1| = |M_2|$, and call the key-dependent round functions $F_1$ and $F_2$.

[Picture at Wikipedia page on Feistel networks, for example, but you need to relabel it.]

12. True. DES would remain invertible—it would still be a blockcipher—even if each S-box (the eight functions $S_1, \ldots, S_8 : \{0,1\}^6 \to \{0,1\}^4$) were replaced by the function $S(x) = x^2 \text{mod} 16$.

A Feistel network gives rise to a permutation for any found function $F$.

13. False. Dog day didn’t work out so well, as there was only one dog, and he wouldn’t stop barking. Extra credit: name the dog(s), or write a limerick about dog day.

That’s crazy; dog day was great! We had Claire, Ki ki, Meyla, Outlaw, and Papillion. Here’s what I recall:

Five dogs came last Friday to class;  
They longed for good crypto, alas.  
“What’s this DES-thing about?  
Its damn key will run out!”  
Yelped a Shepherd quite clearly aghast.

And now for some student solutions (only the first a limerick):

Outlaw came by to dog day.  
He didn’t have much to say.  
He sat in class  
and watched time pass  
until he could go out to play. — Y.O.

Roam like no one is watching.  
Bark like no one is listening.  
Sleep like it is heaven on Earth. — C.J.

The professor was going too fast  
so the dog asked him to paws. — K.L.

The dogs came, the students played,  
not knowing the dogs could help their grades. — M.A.