Midterm Exam

October 21, 1998

Name: _____

1. Soon after DES was introduced as a standard, two main points of criticism against the algorithm were voiced. Each criticism was associated with a potential attack.

   Which were the two initial criticisms brought up against DES? How valid are these criticisms retrospectively, considering today's ability to break DES?

2. In Bruce Schneier's article "Cryptographic Design Vulnerabilities" it is stated that in practical attacks the cryptographic algorithms are rarely the point of failure. Describe some classes of attacks which are more likely to succeed in practice than breaking the underlying encryption algorithm. You are welcome to give examples.

3. At first glance it seems as though an exhaustive key search is possible against a one-time-pad (OTP) system. Given is a short message, let's say five ASCII characters represented by 40 bits, that was encrypted using a 40 bit OTP. Explain exactly why an exhaustive key search will not succeed even though sufficient computational resources are available.

4. We are interested in an affine cipher that encrypts/decrypts messages written with the full German alphabet. The German alphabet consist of the English one together with the three umlauts Ä, Ö, Ü, and the (even stranger) "double s" character ß.

   We use the following mapping from letters to integers:

A ↔ 0	B ↔ 1	C ↔ 2	D ↔ 3	E ↔ 4	F ↔ 5
G ↔ 6	H ↔ 7	I ↔ 8	J ↔ 9	K ↔ 10	L ↔ 11
M ↔ 12	N ↔ 13	O ↔ 14	P ↔ 15	Q ↔ 16	R ↔ 17
S ↔ 18	T ↔ 19	U ↔ 20	V ↔ 21	W ↔ 22	X ↔ 23
Y ↔ 24	Z ↔ 25	Ä ↔ 26	Ö ↔ 27	Ü ↔ 28	ß ↔ 29

   (a) How large is the key space of the affine cipher for this alphabet?

   (b) The following ciphertext was encrypted using the key $(a = 17, b = 1)$. What is the plaintext?

   Ä U ß W ß

   (c) From which village does the solution to 4b come? (1 extra point)

5. The minimum key length for the (to be selected) AES algorithm is 128 bit. Assume that a special purpose hardware key-search machine can test one key in 10 ns on one processor. The processors can be parallelized. Assume further that one such processor costs \$10, including overhead. (Note that both the processor speed and the prize are rather optimistic assumptions.) We assume also that Moore's law holds, according to which processor performance doubles every 18 months.

   How long do we have to wait until an AES key search machine can be built which breaks the algorithm on average in one week and which doesn't cost more than \$1 million?

6. Enclosed is a partial description of DES. A DES key K_w is called a *weak key* if encryption and decryption are identical operations:

$$\mathrm{DES}_{K_w}(x) = \mathrm{DES}^{-1}_{K_w}(x) \quad , \quad \text{for all } x \tag{1}$$

   (a) Describe the relationship of the subkeys in the encryption and decryption algorithm that is required so that (1) is fulfilled.

   (b) There are four weak DES keys. What are they?

   (c) What is the likelihood that a randomly selected key is weak?

7. One major drawback of public-key algorithms is that they are relatively slow. In this problem we study one of the standard acceleration techniques that is available for the RSA cryptosystem.

   Assume that in an implementation of the RSA cryptosystem, one modular multiplication takes twice as much time as modular squaring. How much quicker is one encryption on average if instead of a 1024 bit public key the short exponent $b = 17$ is being used? Assume that the square-and-multiply algorithm is being used in both cases.