MODFIIED VESION OF LAST YEARS FINAL
NOTE: Last Years Final had a problem on it I removed since we did not do that topic this year. Thats why the points do not sum to 100.
This is NOT to hand in. This is a Study Guide.

1. (20 points) No explanations required.

   (a) If Alice and Bob use an alphabet of size 23 then what is the number of affine ciphers?

   (b) If Alice and Bob use an alphabet of size 24 then what is the number of affine ciphers?

   (c) Zelda uses the random string method to share a secret with Alice and Bob so that they can't recover the secret alone but can with each other. Zelda gives Alice the string 10100 and Bob the string 11010. What is the secret?

   (d) What is $2^{65} \pmod 7$?

SOLUTION TO PROBLEM 1

a) $\phi(23) = 22$ so the answer is 22×23.

b) $\phi(24) = \phi(2^3 \times 3) = \phi(2^3)\phi(3) = (2^2) \times (3-1) = 8$ so ans is 8×24

c) Alice and Bob just XOR their strings to get

Alice String: 10100 Bob String: 11010

Answer: 01110

2. (20 points) For each statement below state if its TRUE, FALSE, or UNKNOWN TO SCIENCE. EXPLAIN your answer and be COHERENT, CLEAR, and CONCISE.

   (a) The 1-time pad is UNCRACKABLE!

   (b) The NSA is far ahead of academics in terms of research in cryptography.

   (c) If Eve can crack Diffie-Helman quickly then she can solve discrete log quickly.

   (d) If Eve can solve Discrete Log quickly then she can crack Diffie-Helman quickly.

   (e) Fix p a prime and g a generator. Let $KEY(x, y)$ be the secret key that Alice and Bob will share if they do the Diffie-Helman protocol with Alice picking x and Bob picking y. Then $KEY(x, y) = KEY(y, x)$.

SOLUTION TO PROBLEM 2

(a) The 1-time pad is UNCRACKABLE!

TRUE: All Eve gets is a sequence of Random bits from which she can't learn anything.

(b) The NSA is far ahead of academics in terms of research in cryptography.

FALSE: The NSA is hampered by not being able to talk about their work to a wide circle of people.

(c) If Eve can crack Diffie-Helman quickly then she can solve discrete log quickly.

UNKNOWN TO SCIENCE. Its plausible that Eve cracked Diffie-Helman by being able to go from (g^a, g^b) to g^{ab} without doing discrete log.

(d) If Eve can solve Discrete Log quickly then she can crack Diffie-Helman quickly.

TRUE. Eve sees (g^a, g^b) so if she can find a, b (actually just one of them) then she can compute $(g^a)^b \equiv g^{ab} \pmod{p}$.

(e) Fix p a prime and g a generator. Let $KEY(x, y)$ be the secret key that Alice and Bob will share if they do the Diffie-Helman protocol with Alice picking x and Bob picking y. Then $KEY(x, y) = KEY(y, x)$.

TRUE. $KEY(x, y) = (g^x)^y \equiv g^{xy} \pmod{p}$. $KEY(y, x) = (g^y)^x \equiv g^{yx} \equiv g^{xy} \pmod{p}$.

3. (20 points)

   (a) Alice and Bob use Diffie-Helman with prime p and with a number g that is NOT a generator. Why is this a terrible idea?

   (b) Zelda wants to use the polynomial method for secret sharing. Her friends are named $A_0, A_1, \ldots, A_{100}$. She wants to give A_i the value $f(i)$. Why is this a terrible idea?

SOLUTION TO PROBLEM 4

   (a) Alice and Bob use Diffie-Helman with prime p and with a number g that is NOT a generator. Why is this a terrible idea?

   WHY IS THIS A TERRIBE IDEA? Lets say that g is not a generate. Then there will be some L that divides $p-1$ such that $g^L \equiv 1$. Hence the distinct powes of g are $\{g^1, \ldots, g^L\}$. This could be a VERY small set! When Eve sees g she will test if g is a generator, find out that its NOT. She will then compile a table of (i, g^i) that is SHORT, only L long! This table allows here to compute Discrete log quickly and hence break DH. (NOTE- the key is that L is small. If g IS a generator then $L = p-1$ which is large.)

   (b) Zelda wants to use the polynomial method for secret sharing. Her friends are named $A_0, A_1, \ldots, A_{100}$. She wants to give A_i the value $f(i)$. Why is this a terrible idea?

   WHY IS THIS A TERRIBE IDEA? Person A_0 gets $f(0)$ which IS the secret.

4. (20 points) For each statement below state if its TRUE, FALSE, or UNKNOWN TO SCIENCE. EXPLAIN your answer and be COHERENT, CLEAR, and CONCISE.

   (a) Zelda has a secret s. There is a way for her to share it with $A_1, \ldots, A_{100}$ such that

   (1) if 50 people get together they can decode it

   (2) if 49 people get together they cannot decode it- info-theoretic security

   (3) A_1 gets a string of length $\leq |s|/2$

   (4) everyone else gets a string of length $\leq 2|s|$

   If YES then describe the protocol. If NOT then prove that no such protocol exists. If UNKNOWN TO SCIENCE then you need not explain.

   (b) Zelda has a secret s. There is a way for her to share it with $A_1, \ldots, A_{100}$ such that all of the following hold:

   (1) if 50 people get together they can decode it

   (2) if 49 people get together they cannot decode it- computational security

   (3) A_1 gets a string of length $\leq |s|/2$

   (4) everyone else gets a string of length $\leq 2|s|$

   If YES then describe the protocol. If NOT then prove that no such protocol exists. If UNKNOWN TO SCIENCE then you need not explain.

a) NOT possible! Assume there is a protocol where A_1 gets a string of length $|s|/2$ (I won't need to use anything else). Then we show that SOME information is leaked. If $A_2, \ldots, A_{50}$ get together (thats only 49 people) Gee, if they only had the share from A_1 they would know the secret. But wait- there are ONLY $2^{|s|/2}$ possibilities for that share. So they CAN do the following:

For all x of length $|s|/2$ find out what the secret WOULD be if A_1's share was x. This gives you $2^{|s|/2}$ possibilities for the secret. This IS NOT INFORMATION THEORETIC SECURE since you have learned SOMETHING about the secret.

b) IS possible. See the notes on Secret Sharing with Short Shares and the part about using RSA.

Scratch Paper