CSE 599R, Cryptanalysis, University of Washington

Final Exam
Tuesday, December 9, 2008
John Manferdelli

Please write clearly. Calculators permitted. Have a good holiday!

1. *General Definitions [20].* Define and describe the security requirements (e.g. - what the expected effort is to "break" a properly designed instance of) each of the following:
    a. Block cipher
    b. Public key cipher
    c. Cryptographic hash
    d. Diffie-Hellman key exchange

2. *Block Ciphers [20].*
    a. Let V= $GF(2)^n$ and f: V → GF(2). The normalized Walsh transform of f is defined as $F(\mathbf{w}) = 2^{-n} \sum_{\mathbf{x}\in V} (-1)^{\mathbf{w}\bullet\mathbf{x}+f(\mathbf{x})}$. Let $a_\mathbf{w}$ be the number of arguments, **x**, for which the linear function **w•x** and f(**x**) agree. Calculate the value of a_w in terms of F(w). What does this say about the best affine approximation for f?
    b. Can f always be represented as a polynomial over $GF(2)[x_1, x_2,…, x_n]$? Why?
    c. If f is "random", how many monomials are likely to be in the algebraic representation of f as a polynomial over $(x_1, x_2,…, x_n)$? What is the probability that this representation contains the constant term 1?
    d. *Extra Credit:* Suppose E(**k, x**): $GF(2)^n \times GF(2)^n$ → $GF(2)^n$ is a block cipher. For notational convenience, set V= $GF(2)^n$. As a crack cryptographer, you discover each bit position of E(**k, x**) can be written as a polynomial in the **x**=$(x_1,…,x_n)$ with coefficients from GF(2)[**k**] with the following property[1]: $\pi_i(E(\mathbf{k}, \mathbf{x})) = \sum_{\alpha\in V} g_{\alpha,i}(k_1,…,k_n)\, \mathbf{x}^\alpha$. When non-zero, the $g_{\alpha,i}(k_1,…,k_n)$ are very complex polynomials (about $2^{n/2}$ terms) in the key variables but, for each i, only about 2n of the coefficients, $g_{\alpha,i}(k_1,…,k_n)$, are non-zero. For a fixed key, how could you break this with known corresponding plain and cipher text? How much of it would you need? How long would it take?

[1] Remember, if $\mathbf{x}=(x_1, …, x_n)$ and $\alpha=(\alpha1,…,\alpha n)$, $\mathbf{x}^\alpha$ means $x_1^{\alpha1}\, x_2^{\alpha2} … x_n^{\alpha n}$. $\pi_i(\mathbf{x}) = x_i$.

3. *DES [20].*

   a. DES (pictured in Figure 1) is a Feistel cipher which maps a 64-bit input (the plaintext) to a 64-bit output (the ciphertext). It is composed of (1) an "initial permutation" of the 64-bit input, IP, (2) a key schedule, KS, which produces 16 48-bit round keys from a 56-bit master key and two basic transformations (3) τ, which exchanges two 32 bit quantities [τ(L,R)= (R,L)] and (4) $\sigma_{K[i]}$(L,R)= (L$\oplus$f(E(R)$\oplus$K[i]), R), where K[i] is the round key for round i. Referring to Figure 1, write DES as a composition of these transformations. Imagine the key schedule is given, so you do not have to write how any K[i] is obtained.
   b. Given this representation, argue that for a fixed key, **k,** DES$_{\mathbf{k}}$(**x**) is a bijection. Write down the inverse (ciphertext to plaintext) in terms of the foregoing transformations.
   c. Describe the notions of confusion and diffusion and explain which cryptographic elements in DES provide each.
   d. Bob is a veteran programmer in the security group of a large software company and doesn't like new things like AES. He designs his own cipher from DES which takes a 128 bit input block to a 128 bit output block (just like AES) and uses a 112 bit key, K. Here's Bob's scheme: He picks three *invertible* linear transformations L_1, L_2, L_K. L_1 and L_2 map GF(2)^{128} → GF(2)^{128} and L_K maps GF(2)^{112} → GF(2)^{112}. For convenience of notation, we write **x**=($\mathbf{x_1}$, $\mathbf{x_2}$) and **k**=($\mathbf{k_1}$, $\mathbf{k_2}$) where is **x** a 128 bit vector in GF(2)^{128} composed of two 64 bit vectors $\mathbf{x_1}$, $\mathbf{x_2}$ and **k** is a 112 bit vector in GF(2)^{112} composed of two 56 bit vectors $\mathbf{k_1}$, $\mathbf{k_2}$. Given the key **k** and input **x**, Bob encrypts using the following algorithm:
      1. Compute ($\mathbf{x_1}$, $\mathbf{x_2}$) =L_1(**x**) and ($\mathbf{k_1}$, $\mathbf{k_2}$) = L_K(**k**).
      2. Compute $\mathbf{y_1}$=DES($\mathbf{k_1}$,$\mathbf{x_1}$) and $\mathbf{y_2}$=DES($\mathbf{k_2}$,$\mathbf{x_2}$).
      3. Compute the output of the cipher **z**= L_2($\mathbf{y_1}$, $\mathbf{y_2}$).

Bob reasons this cipher is secure because (1) there is a 112 bit key, (2) the cipher mixes input bits with L_1 and output bits with L_2, and (3) the cipher mixes key bits with L_K . The cipher is invertible because L_1 and L_2 are so it can be decrypted in the obvious way. DES is a pretty good cipher and Bob thinks he will save his software company lots of money since they have spent years coding DES (don't laugh). What is the security of Bob's system? How much better does it get if L_1, L_2 and L_K are *invertible* non-linear transformations?

4. *RSA [20].*
    a. Describe the RSA cryptosystem.
    b. Using p=37, and q= 41, and e= 7, specify the public key and encipher M= 11 using the public key. Show your calculations and be sure to exponentiate in an efficient way.
    c. For the parameters in b, knowing the private factors, calculate the decryption exponent d which insures that M^{ed}=M (mod n). Now verify the private keyholder can recover M in this case.
    d. How hard is it to find large primes (about one thousand bits)? How would you do it?

5. *Mostly Elliptic Curve [20].*

   a. Describe the discrete log and elliptic curve El Gamal cipher system. Why do you believe it is safe?

   b. Derive the formula for adding two points with different x-coordinates on E(a,b) over the rational numbers. Does the same formula apply to $E_p(a,b)$: $y^2=x^3+ax+b \pmod p$?

   c. What is a singular curve? Is the curve $E_{23}(1,1)$: $y^2=x^3+x+1 \pmod{23}$ singular[2]. Let P_1= (3, 10), P_2= (11, 20), P_3= (3, 13), calculate P_1+P_2 and P_1+P_3. What is 7(12, 19)? *Extra credit:* Can you guess the order (#E) of the group now?

   d. Estimate the size of the elliptic curve group in the foregoing problem. What is the relation between the size of the elliptic curve group (i.e.-the points on the curve and O) and the order of a point?

The End

[2] Hint: What does $D=4a^3+27b^2$ have to do with being singular?

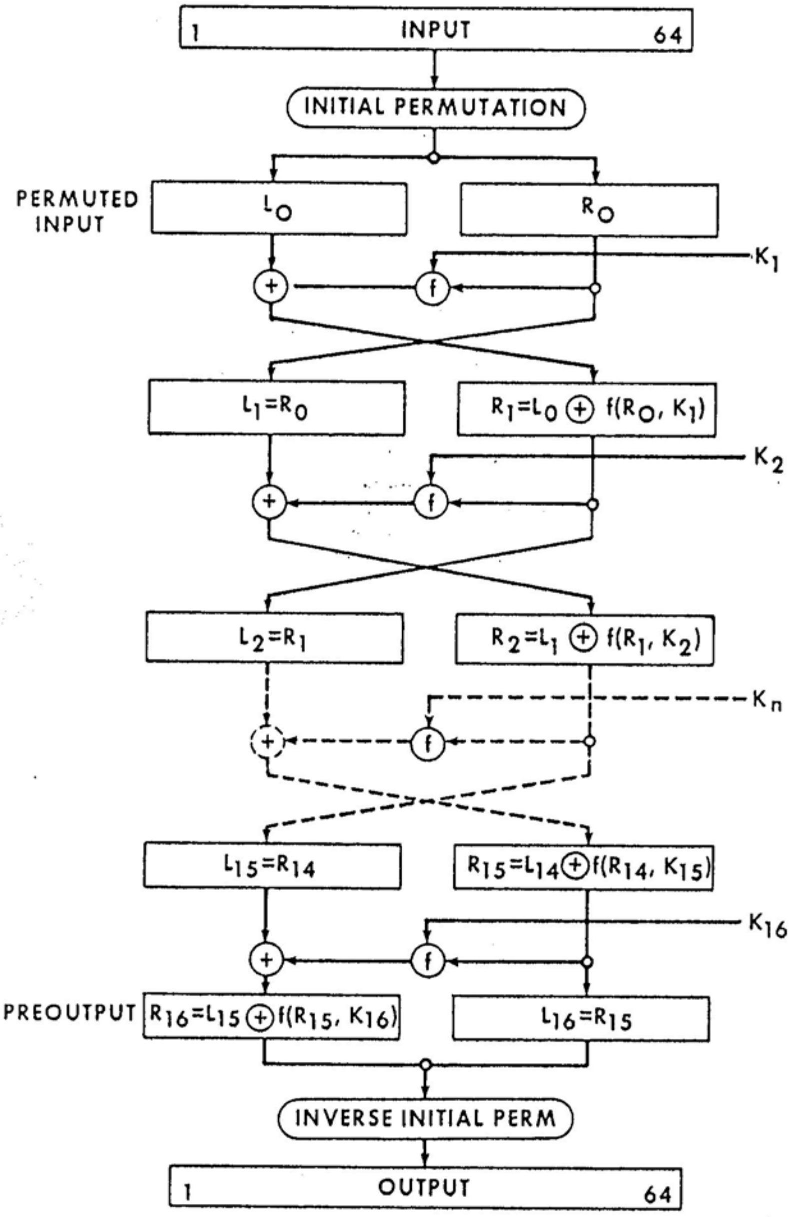
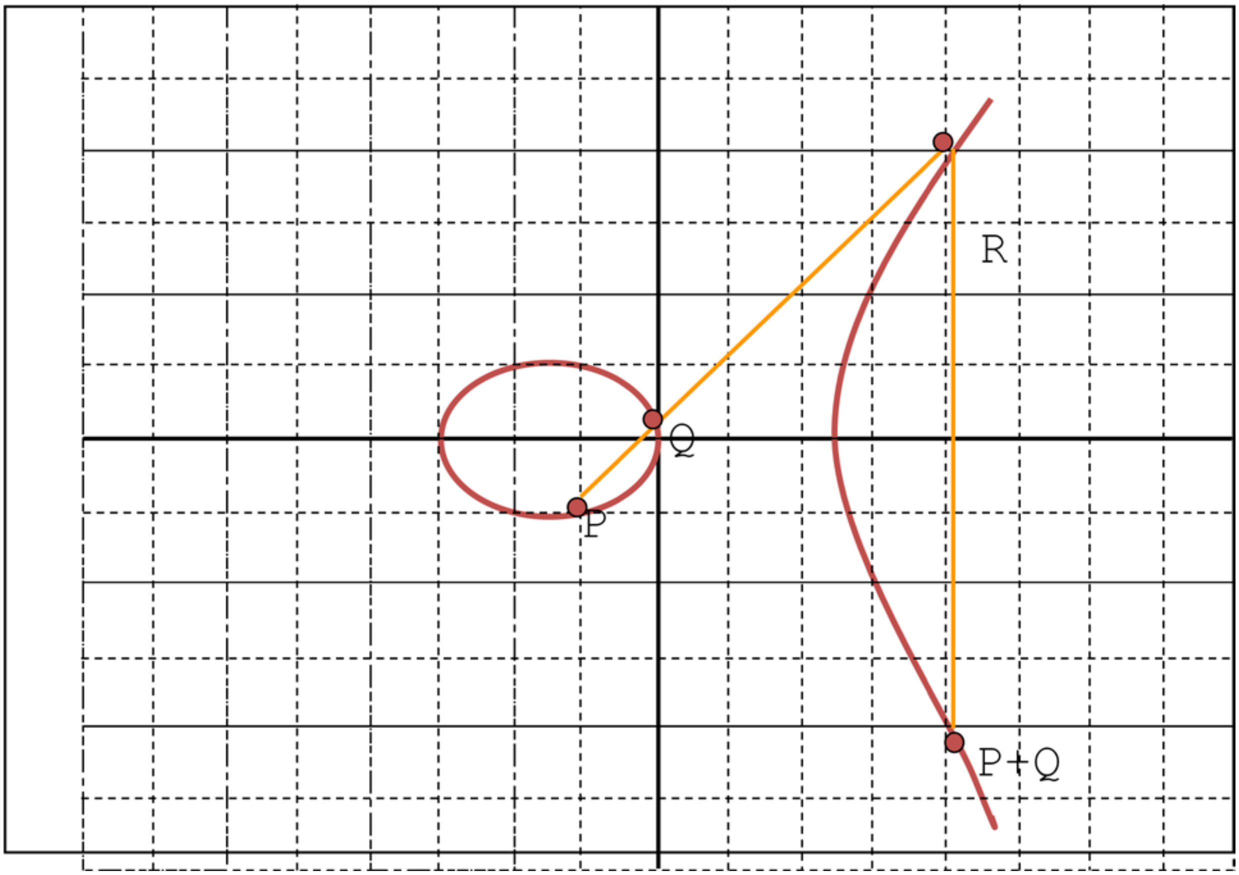


Figure 5.1. Electronic Codebook (ECB) Mode—Enciphering Computation.

Figure 1: DES from FIPS-46

First Aid



Given two points P and Q lying on the curve $E_R(a, b)$: $y^2=x^3+ax+b$, where $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ then $P+Q=R=(x_3, y_3)$ where:

- If $x_1 \neq x_2$, $m=(y_2-y_1)/(x_2-x_1)$, and
    - $x_3 = m^2 - x_1 - x_2$
    - $y_3 = m(x_1 - x_3) - y_1$
- If $x_1=x_2$ and $y_1 \neq y_2$, then $y_1=-y_2$ and P+Q=O, Q= -P
- If $x_1=x_2$ and $y_1=y_2$, then P=Q, R=2P, $m=(3x_1^2+a)/(2y_1)$, and
    - $x_3 = m^2 - x_1 - x_2$
    - $y_3 = m(x_1 - x_3) - y_1$