CSC474/574 - Information Systems Security: Homework1 Solutions Sketch

February 20, 2005

1. Consider slide 12 in the handout for topic 2.2. Prove that the decryption process of a one-round Feistel cipher is the same as the input of the corresponding encryption process. That is, $(L'_2, R'_2) = (L_0, R_0)$.
   Ans.

   $$R_0 = L_1 = R_2 = R'_0 = L'_1 = R'_2$$
   $$L'_2 = R'_1 = L'_0 \oplus (R'_0, K_1) = L_2 \oplus (R_2, K_1) = R_1 \oplus (R_0, K_1) = L_0$$

2. Random J. Protocol-Designer has been told to design a scheme to prevent messages from being modified by an intruder. Random J. decides to append to each message a hash of that message. Why doesn't this solve the problem?
   Ans. Anybody can generate and append a hash to any message. A malicious adversary can easily modify the message and append the recomputed hash value. This modification goes undetected at the receiving end.

3. How many DES keys, on the average, encrypt a particular plaintext block to a particular ciphertext block?
   Ans. There are 2^{56} possible keys and 2^{64} possible ciphertext blocks for a particular plaintext block. So only about $2^{56-64} = 1/256$ of the possible ciphertext blocks can be obtained with a DES key.

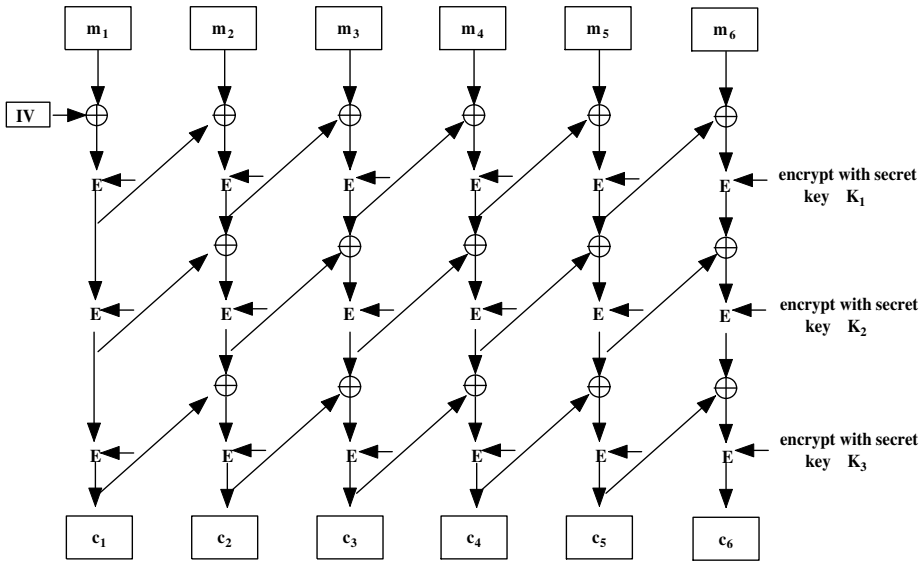
4. Alice developed a message authentication code (MAC) based on DES. Her algorithm works as follows: For a given input message M, represent M as $M = (X_1||X_2||\ldots||X_m)$, where X_i is a 64-bit block and $||$ represents concatenation. Compute $Delta(M) = X_1 \wedge X_2 \wedge ... \wedge X_m$, where $\wedge$ represents bit-wise XOR. Then the MAC for M is computed as $C_K(M) = E_K(Delta(M))$, where E is DES encryption algorithm and

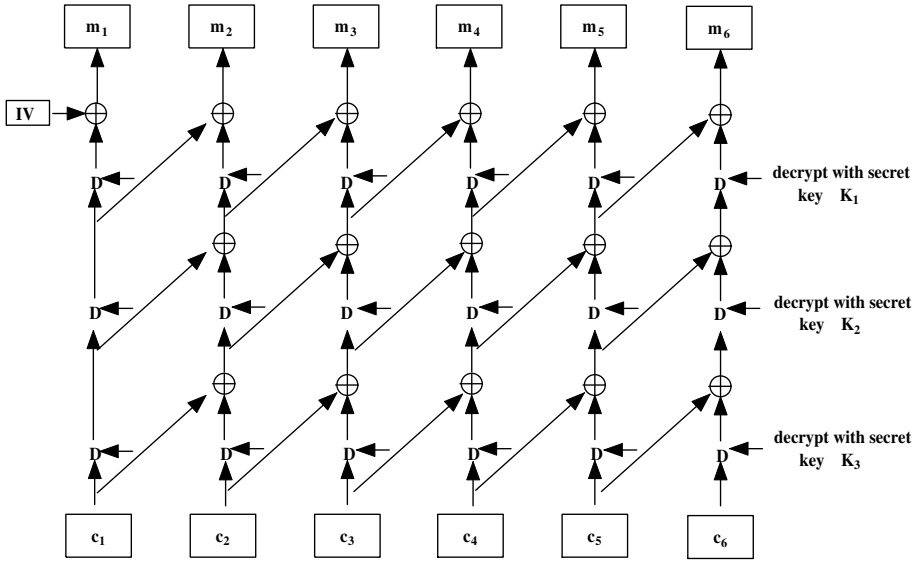
K is the secret key. Unfortunately, this scheme is vulnerable. Describe an attack against it.

Ans. A possible attack on this scheme could be a word reordering attack. A reordering attack is possible because it yields the same hash as the original message. An intruder can easily create a message M and compute $W = Delta(M) \wedge Delta(M')$ where $Delta(M'||W) = Delta(M)$.

5. Let's assume that someone does triple encryption by using EEE with CBC on the inside. Suppose an attacker modifies bit x of ciphertext block n. How does this affect the decrypted plaintext? (See Figure 4-16 and related text for triple EDE DES with CBC on the inside. But note that the question is about triple EEE DES with CBC on the inside)

   Ans. Triple encryption using EEE with CBC on the inside is three successive CBC encryptions: Decryption is the inverse operation:





From this it can be seen that a modification to ciphertext block n propagates to plaintext blocks n through $n+3$. No other plaintext blocks are affected.

6. How do you decrypt the encryption specified in 5.2.3.2 Mixing In the plaintext?

   Ans. The decryption process proceeds as follows:

$$
\begin{aligned}
b_n &= MD(K_{AB}|c_n - 1) \\
b_{n-1} &= MD(K_{AB}|c_{n-2}) \\
&\dots \\
b_{n-i} &= MD(K_{AB}|c_{n-i-1}) \\
&\dots \\
b_2 &= MD(K_{AB}|c_1) \\
b_1 &= MD(K_{AB}|IV)
\end{aligned}
$$

$$
\begin{aligned}
p_n &= c_n \oplus b_n \\
p_{n-1} &= c_{n-1} \oplus b_{n-1} \\
&\dots \\
p_1 &= c_1 \oplus b_1
\end{aligned}
$$

   In short, knowing KAB, c_i and IV, b_i can be generated. Then it is

easy to compute $p_i = c_i \oplus b_i$

7. A and B want to establish a secure communication channel between them. They do not care about the confidentiality of the messages being transmitted, but they do want to ensure the integrity and authenticity of the messages. Answer the following questions by drawing diagrams that show the procedures of sending and receiving messages. Assume A and B share a common key K.

   (a) How can they achieve their goal only with secret key cryptography?
   Ans. Sender $\rightarrow$ Recipient : $M||E_K(M)$

   (b) How can they achieve their goal only with hash function (e.g., MD5)?
   Ans. Sender $\rightarrow$ Recipient : $\{M||E_K(H(M))\}$

   (c) Can they get non-repudiation? (2 points) If yes, how? If no, why?
   Ans. No, it is not possible to achieve non-repudiation with the help of just a commonly shared key because a sender can repudiate a previously authenticated message by claiming that the shared secret was somehow compromised. It is also possible that the recipient who has a copy of the shared secret key might have forged the signature.

   (d) Describe a way A and B can get non-repudiation. Explain your assumption and draw a diagram to show the procedure.
   Ans. Using digital signatures

8. The DSA algorithm requires a random number each time a digital signature is generated. Demonstrate that the DSA algorithm is vulnerable if this random number is used twice.
   Ans. If $k_1 = k_2$, then $r_1 = r_2$ and $s_1 = [k^{-1}(H(M_1)+xr)] \mod q$ and $s2 = [k^{-1}(H(M_2)+xr)] \mod q$. Then $k = (s1-s2)^{-1}[H(M_1)H(M_2)] \mod q$. So the private key x can be obtained from s_1 or s_2 above.

9. Manually complete the following operations. Explain your reason for each step.

   (a) $1234^{16} \mod 17$

   $$1234^{16} \mod 17 = 1$$

since 17 is a prime and $gcd(1234, 17) = 1$ we can use Fermat theorem.

(b) $54^{51} \mod 17$

$$54^{51} \mod 17 = (54 \mod 17)^{(51 \mod 16)} \mod 17 = 3^3 \mod 17 = 10$$

since 17 is a prime and $gcd(54, 17) = 1$ and $\phi(17) = 16$

(c) $53^{97} \mod 51$

$$\begin{aligned} 53^{97} \mod 51 &= (53 \mod 51)^{(97 \mod \phi(51))} \mod 51 \\ &= 2^{(97 mod (17)\phi(3))} \mod 51 \\ &= 2^{(97 \mod 32)} \mod 51 \\ &= 2^1 \mod 51 = 2 \end{aligned}$$

(d) $gcd(33, 121)$

$$\begin{aligned} gcd(33, 121) &= gcd(121, 33) = gcd(33, 22) = gcd(22, 11) \\ &= gcd(11, 0) = 11 \end{aligned}$$

(e) $2^{-1} \mod 17$

$$2^{-1} \mod 17 = -8 \mod 17 = 9$$

using the extended Euclid algorithm, $Y3 = 1 = gcd(2, 17)$ and $Y2 = -8 = 2^{-1} \mod 17$

(f) $\log_{2,5}(4)$

$$\log_{2,5}(4) = 2$$

since:

$$\begin{aligned} 2^0 \mod 5 &= 1 \\ 2^1 \mod 5 &= 2 \\ 2^2 \mod 5 &= 4 \\ 2^3 \mod 5 &= 3 \\ 2^4 \mod 5 &= 1 \end{aligned}$$

Another method is to solve for x from $2^x \mod 5 \equiv 4 \mod 5 \equiv 22 \mod 5 \Rightarrow x = 2$

10. Consider the polynomial $x^{p-1} = 1(\mod p)$, where p is a prime number. It has at most $p-1$ roots (because it is a polynomial of degree $p-1$). Show exactly the roots of this polynomial using Fermat Theorem.
Ans. Roots of $x^{p-1} = 1(\mod p) = \{1, 2, 3, ..., p-2, p-1\}$. According to Fermat theorem, $x^{p-1} = 1(\mod p)$ for all x such that $gcd(x, p) = 1$, and since p is prime, $1 \leq x \leq p-1$ are relative primes to p.

11. Assume that p is a prime number and a is a positive integer not divisible by p. Prove that $\{a \mod p, 2a \mod p, \ldots, (p-1)a \mod p\} = \{1, 2, ..., (p-1)\}$.
Ans. Assume $\{a \mod p, 2a \mod p, \ldots, (p-1)a \mod p\} \neq \{1, 2, ..., (p-1)\}$. Then there exists x and y in $\{1, 2, \ldots, (p-1)\}$ such that $x \neq y$ and $xa \equiv ya(\mod p)$. i.e., $xa = ya + kp$ and can be rewritten as $(x-y)a = kp$. Factoring left side yields $p_1^{m_1}...p_k^{m_k} = kp$ Then since a is not divisible by p, p is not on the left side which contradicts that p is on the right side. So we can prove that $\{a \mod p, 2a \mod p, \ldots, (p-1)a \mod p\} = \{1, 2, \ldots, (p-1)\}$.