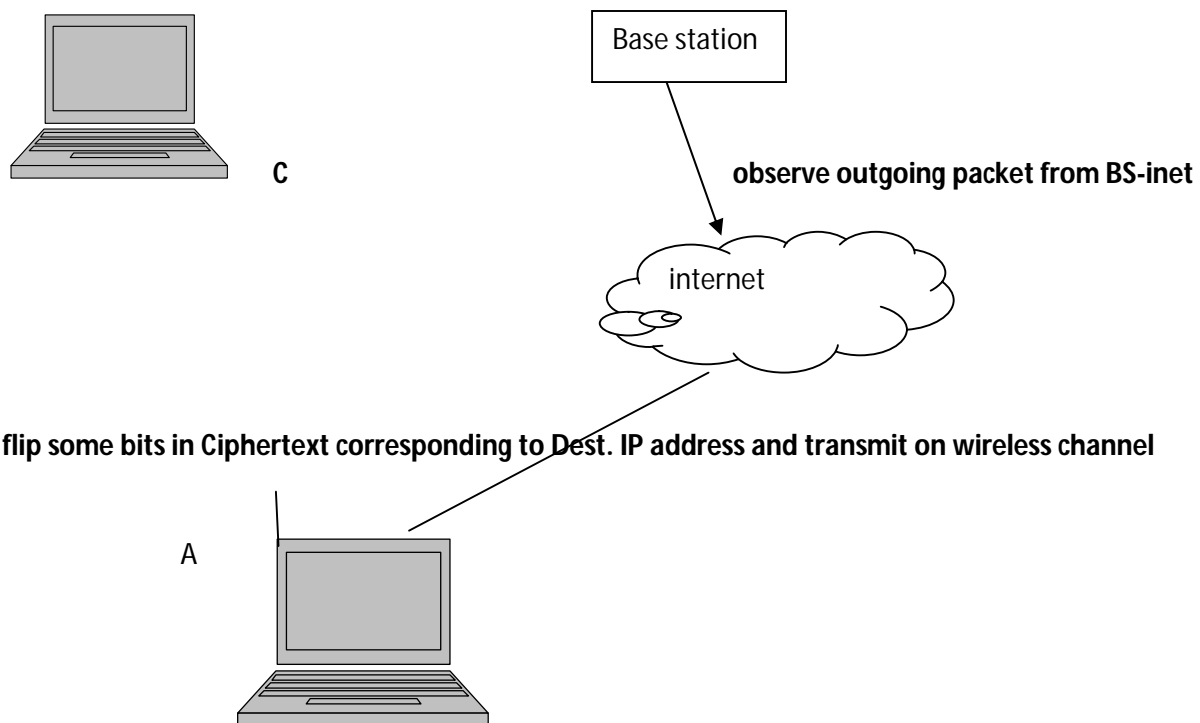


## CSE 508 NETWORK SECURITY

9/14/2009

### TOPIC COVERED

- 1) BASE STATION AS DECRYPTION ORACLE
- 2) Theorem about composition of 2 pseudo Random Generators to produce large random sequence from a small seed with minimal increase in Advantage
- 3) Lemma on Concatenating 2 pseudo random generators



### Base Station as Decryption Oracle

We have seen in previous lecture how Base station can work as encryption oracle

#### **Base station can also work as Decryption Oracle**

Suppose Attacker is Base Station's ISP

We can attack using the following steps

1. Flip some bits in ciphertext corresponding to destination IP address
2. Transmit new ciphertext on wireless channel

3. Observe outgoing packet from base station to internet

Note- if attacker is ISP we don't care what destination IP address is.

**Definition**

$G: \{0,1\}^l \rightarrow \{0,1\}^L$  is a  $t, \epsilon$  secure pseudo random generator if

$$G(U_l) \stackrel{t, \epsilon}{\sim} U_L$$

**Theorem:** If  $G_1: \{0,1\}^l \rightarrow \{0,1\}^L$  is  $t, \epsilon_1$  secure Pseudo random generator and  $G_2: \{0,1\}^L \rightarrow \{0,1\}^M$  is  $t', \epsilon_2$  Secure running in time  $t'$ , then  $G_2 \circ G_1$  is  $t-t', \epsilon_1 + \epsilon_2$  secure Pseudo Random Generator

Note :  $t$  corresponds to time to break  $G_1, G_2$   $t'$ : time to execute  $G_2$

**Proof:** By definition

$$U_L \stackrel{t, \epsilon_1}{\sim} G_1 \circ U_l$$

By Data Processing Inequality

$$G_2 \circ U_L \stackrel{t-t', \epsilon_1}{\sim} G_2 \circ G_1 \circ U_l$$

By Definition

$$G_2 \circ U_L \stackrel{t, \epsilon_2}{\sim} U_m$$

By Transitivity

$$U_m \stackrel{t-t', \epsilon_1 + \epsilon_2}{\sim} G_2 \circ G_1 \circ U_l$$

Hence  $G_2 \circ G_1$  is  $t-t', \epsilon_1 + \epsilon_2$  secure Pseudo Random Generator

**Lemma**

$G_1^{l_1 \rightarrow L_1}$   $t_1, \epsilon_1$  secure runs in  $t_1'$  and

$G_2^{l_2 \rightarrow L_2}$   $t_2, \epsilon_2$  secure runs in  $t_2'$ .

$G_1 || G_2$  is  $t_3, \epsilon_1 + \epsilon_2$  secure where  $t_3 = \text{poly}(t_1, t_2)$

$$G_1 \circ U_{l_1} \stackrel{t_1, \epsilon_1}{\sim} U_{L_1}$$

Using the function in data processing inequality

$$F(x) = x \parallel G_2(U)$$

$$\text{Hence } G_{1 \circ} U_{11} \parallel G_{2 \circ} U_{12} \stackrel{t_1 - t_2'}{\tilde{\varepsilon}_1} U_{L1} \parallel G_{2 \circ} U_{12}$$

$$U_{L1} \parallel G_{2 \circ} U_{12} \stackrel{t_2}{\tilde{\varepsilon}_2} U_{L1} \parallel U_{L2} (= U_{L1+L2})$$

By transitivity

$$G_{1 \circ} U_{11} \parallel G_{2 \circ} U_{12} \stackrel{\min(t-t', t_2)}{\varepsilon_1 + \tilde{\varepsilon}_2} U_{L1+L2}$$