Charles Sturt University

# Master of Information Systems Security

## ITC593 Network and Computer Security

Charles Sturt University

# Week One

- Understand the general model of security
- Substitution Permutation Networks (SPN)
- Feistel Network
- DES And AES

Charles Sturt University

# Week Two

- Electronic codebook mode (ECB).
- Cipher block chaining mode (CBC).
- Cipher feedback mode (CFB).
- Output feedback mode (OFB).
- Counter mode (CTR).

Charles Sturt University

# Week Three

- Understand rijndael algorithm
- Differential Cryptanalysis Attack
- Linear Cryptanalysis Method

Charles Sturt University

# Week Four

- Hash Function and Random Oracle model What are hash func6ons used for (incryptography)?

Charles Sturt University

# Week Five

- Digital Signature
- Public key cryptography ElGamal
- Security notions
- Kerberos and PKI (Public Key Infrastructure).

Charles Sturt University

# Week Six

- Suppose that F: {0,1}n → Zp where P is a large prime and n>P. Proof that f(x)= gx mod (p) is not second pre-image resistant, where g is a generator of Zp. What is the security assumption you use, if to make it pre-image resistant.
- Suppose that f :{0,1}m is a pre{image resistant bijection. For given x E {0,1}2m, write x = x’||x’’, where x’,x’’ E {0,1}m. Then define h :{0,1}2m →{0,1}m as h (x)= (x’Xor x’’). Prove that the function h(x) is not second pre-image resistant.

Charles Sturt University

# Week Six

- The RSA cryptosystem satisfies a multiplicative property: EK(x1)EK(x2) (mod n) = EK(x1x2 (mod n)) : Show that because of this property the RSA cryptosystem is insecure against a chosen ciphertext attack. In particular, given a ciphertext y, describe how to choose a ciphertext y0 such that knowledge of the plaintext x0 = DK(y0) allows the attacker to determine x = DK(y).

- Show that the active CCA against ElGamal encryption not work when against the CramerShoup encryption.

Charles Sturt University

# Week seven

- Assume an elliptic curve with points whose coordinates P = (x; y) satisfy the following congru ence y2 = x3 + x mod 23. Given two points P = (9; 5) and Q = (11; 10), what are the points P + Q, P + P, and Q + Q?
- Let p = 41. Choose a generator for GF(41). Choosing appropriate private, and ephemeral keys, perform the following on the message m = 11, or the next ppropriate message: (a) Encryption using ElGamal. (b) Encryption using semantically security ElGamal. (c) Signing using ElGamal. You can use Pari/GP.

# Week Eight

- Understanding Side-channel attack
- Understanding S-box, EBC, public and private key encryption