BAO MAT THONG TIN

1. Gioi thieu

* Bao mat thong tin

+ Suc manh

+ Giau tin

+ Ma hoa: doi xung symmetrickey 1 khoa (co dien, hien dai: AEF), bat doi xung Asymmetric Key (RSA, ECC), hash (MD5, SHA) -> ma hoa toan ven du lieu, chu ki so, trao doi khoa, chung thuc

1. Ma hoa AES

M -> block0(128 bit)…blockn(128 bit)

Blocki dua vao thuat toan AES

+ Dau vao Preroudtrans(Si, K0)

+ For I = 1 .. n

+ End For

Output: S\*i

1. Ma hoa bat doi xung (Asymmetric-Key C)

Rabin

ElGamal

Eliptic Curve Cryptosystems