Final Exam Review

E1 Stuff (Classical)

SHIFT
AFFINE
GCD, EEA
MOD INVERSE
SUBSTITUTION
VIGENERE
IC, MIC
PLAYFAIR
ADFGVX
HILL
INV 2×2 MATRIX
ENIGMA

Last Stuff

Hash Functions
Weak vs Strong Collision Resistance
Birthday Paradox
log of products
El-Gamal Digital Signature Scheme
Message Authentication Idea
Digital Signature Idea
Quantum Crypto Idea

2 SHEETS OF NOTES FRONT + BACK (11" × 8.5")

NO CALCULATOR

E2 Stuff (Symmetric/Private Key)

bitwise operators
DES
AES

E3 Stuff (Public Key)

Number Theory
Prime Testing - Miller Rabin
ϕ function, Fermat's Thm
Euler's Thm, Discrete Log Problem
Diffie-Hellman, RSA, El-Gamal, ECC - how to add pts.

Fermat Factoring!

* 1 CODING QUESTION *