

PROGRAMMA DIDATTICO ELEMENTI BASE ED INTRODUZIONE ALLA CRITTOGRAFIA

DOCENTE: Dott. Nanni Bassetti

ORE: 4

PROGRAMMA

DEFINIZIONE DI CRITTOGRAFIA

CENNI STORICI

ESEMPI SUI CIFRARI STORICI (ATABASH, CESARE, ALBERTI, ecc.)

APPROFONDIMENTO SUL CIFRARIO DI VIGENERE

SIMULAZIONE IN PYTHON

CONCETTO DI PASSWORD E CHIAVE DI CRIPTAZIONE

HASH E SALT

KEY DERIVATION FUNCTION E KEY STRETCHING

SIMULAZIONE IN PYTHON

CENNI DI CRITTOANALISI (KASISKY E PRINCIPIO DI Kerckhoffs ecc.)

ALGORITMO RSA A DOPPIA CHIAVE

SIMULATORE IN PYTHON

FIRMA DIGITALE

SIMULATORE IN PYTHON

ESPERIMENTO SU TRUECRYPT MODIFICATO