Asymmetric cryptography. AWCe 806 PKA, SKA PKB, SKB publickey Secret Key $Dec(SK_B,C)=M$ known to Known Eve everyone Enc(PKB,M)=C Correctness Syntax: Keygen() → (PK,SK) YM, YSK, PK & Keygen(), CE Enc(PK,M); Dec(SK,C)=M Enc(PK, m) → C Dec (SK, C) → M f(x)= x No, easy to sheet f(x)=1 No, any x leads to 1 Securty: f(X)= Ex (X)) YES because it is [One-way functions] A function f is one way if indisti. from random (1) Given X, it is easy to compute fox) permetation (2) Given y, it is hard to find any x s.t. f(x)=y.

Ex is indinstruguished from a random permutation

Ex 79 x R

x, Ex(x)=y.

Discrete Logarithm Problem (DLP) $f(x) = g \times \text{mod } p$ where p is a large prime (2048 bits long) g is a random value in [219-1] Assumption: John is OWF Easy to compute: Say X is 2048-bit large number. rejected squanty

2 vult
2 · 2 · 2 · 2 · .

Key Exchange (1976) (Tunng award) Clarge primus p, 1292pt Alia b € {1,--, p-2} a < { and, -p-27 $B
eq g^b \mod p$ public A = gamadp pellie $A^b = a^b \mod p$ Ba = gab madp Symmetric - Key encryption communication using k Eve sees: $A = g^a \mod p \implies cannot compute a { cannot compute gab}$ $B = g^b \mod p \implies cannot compute b$ ASSumption: you cannot break DLP (DLP is OWF) < necessary Adv four cannot compute gas mad p from ga, ga, go mad p

Man in the middle attack (MITM) Changel # 1 Malice Alice grodp Bob Ms, 9 modp ~ gbmodp mood p phone on code Channel #2 Slarg out of bound/defleunt Chamel Assumes Adu does not control both Charrels

Public-key encryption Enc(PKB, m) Alice 1. KeyGen() → (PK, SK) 2. Enc(PK, m) + C Dec(SKB,C)=M 3. Dec (SK, C) -om Correctness: FPK, SK = KeyGen, Ym, C=Enc(PK, m) Dec(SK, C) = M Security: similar in spirit m IND-CPA

L Semantic Security KeyGen() → PKISK chooses a message at random Enc(PK, Mb) be# {0,13 of Adv,

Pr [cAdv wins (6=6)] ≤ 1/2 + negl

El Gamal Cryptosystem (1985)
Keygen () — generate \$ a large prime p (2048-bit) ~2 — g ∈ [21p-1]
- generate in a lange prima p (2010) - g & [21p-1]
- $g \in [21P^{-1}]$ - generate \$1 a secret Key $k \in [21P^{-2}]$ 5k
- PK=g mod p ;(g;p public)
Publish PK, Keep SK secret
Due to the DLP assumption, cannot guess "
Enc (RK, m). ME [13-1PT] Discrete Log Marketin
The state of the s
C = (g' mod p; m. PK mod p) (g.p.g. C., C.)
Dec(5K, C1; C2): C2 mod p=m
m. (g modp) modp modp modp correctness
Wifections