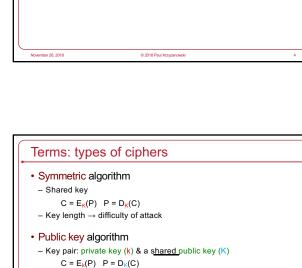


Cryptography: what is it good for? Confidentiality others cannot read contents of the message Authentication others origin of message Integrity verify that message has not been modified





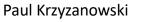
© 2018 Paul Krzy.



 $C = E_{k}(P) P = D_{k}(C)$

Confidentiality

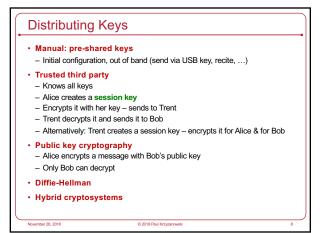
```
EncryptionPlaintext (cleartext) message PEncryption E(P)Produces Ciphertext, C = E(P)Decryption, P = D(C)Cipher = cryptographic algorithm
```



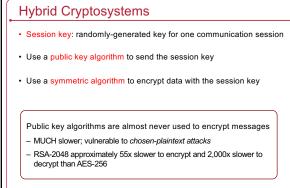
ber 26, 2018

Key distribution

Secure key distribution is the biggest problem with symmetric cryptography



Diffie-Hellman Key Exchange Key distribution algorithm - First algorithm to use public/private "keys" - Not public key encryption - Uses a one-way function Based on difficulty of computing discrete logarithms in a finite field compared with ease of calculating exponentiation - Compute common key = f(your_private_key, their_public_key) - Eavesdroppers cannot compute this





Hash functions

- Cryptographic hash function (also known as a digest) – Input: arbitrary data
- Output: fixed-length bit string
- Properties of a cryptographic hash, *H=hash(M)*:

– One-way function

- Given H, it should be difficult to compute M
- Collision resistant
- Given *H*, it should be difficult to find *M'*, such that *H=hash(M'*)
 For a hash of length L, a perfect hash would take 2^(L/2) attempts

Efficient

• Computing H should be computationally efficient

