PUmal
Browser
Malicious
www.bank.com
U
M
S
PUbank
Initial unencrypted exchange
Initial unencrypted exchange
PUmal
public key of M sent to browser
public key of server sent to browser
PUbank
Encrypted with PUmal
Encrypted with PUbank
Ks
Ks
Ks
Encrypted with Ks
Src=U
Dst=S
Data
x%6kQ2#...4Tre
Can decrypt all data
Src=S
Dst=U
Data
jsd893f#1(lU12
...
^jsa,U3V−!df