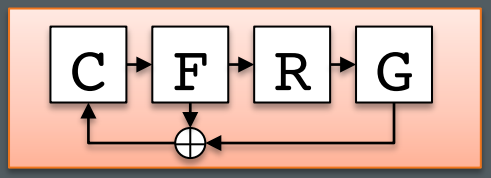
Rump Session 2016

Crypto Forum Research Group

Kenny Paterson

RHUL



Crypto Forum Research Group

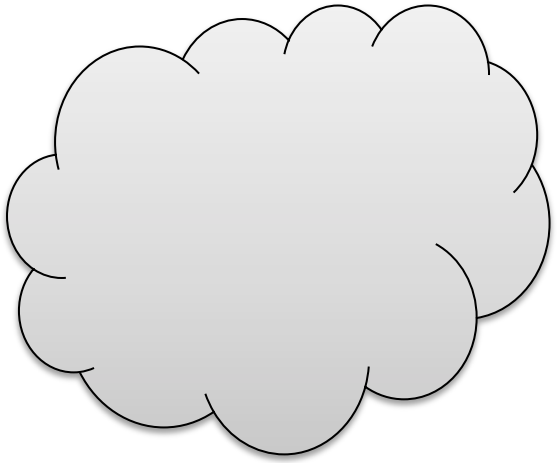
Kenny Paterson

Information Security Group

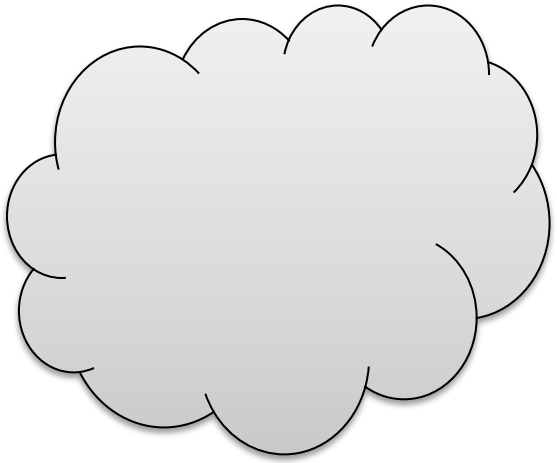
@kennyog; www.isg.rhul.ac.uk/~kp

ROYAL HOLLOWAY UNIVERSITY OF LONDON

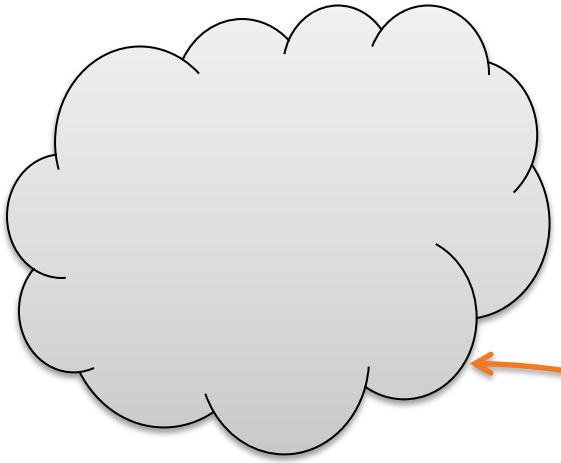
IETF/IRTFCFRG (Acronym Soup)



IETF/IRTFCFRG (Acronym Soup)



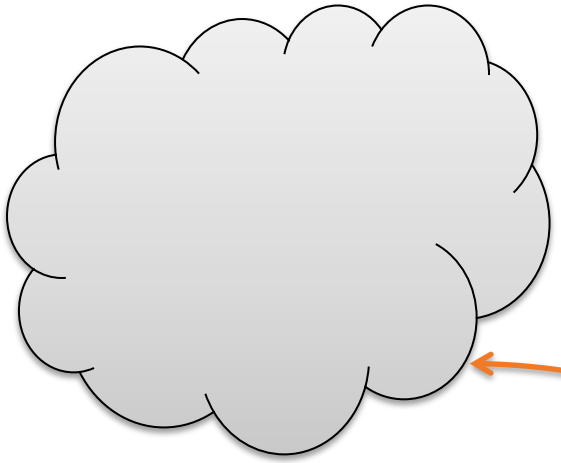
IETF/IRTFCFRG (Acronym Soup)

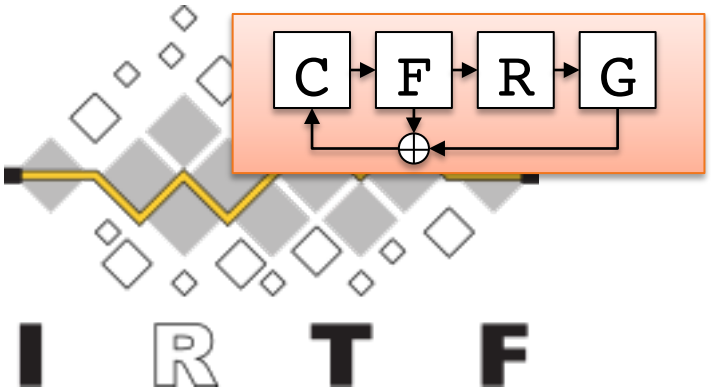


Objective:

make this work!

IETF/IRTFCFRG (Acronym Soup)

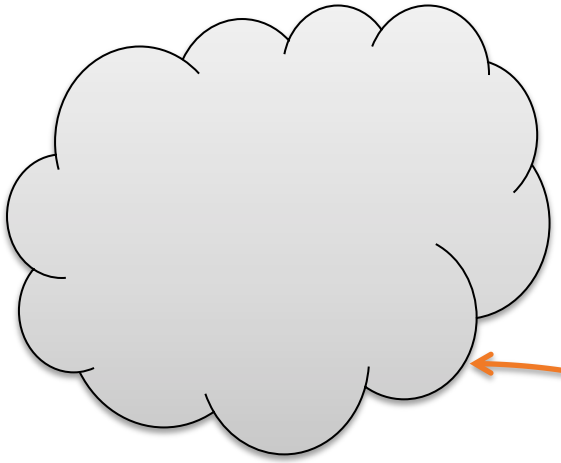


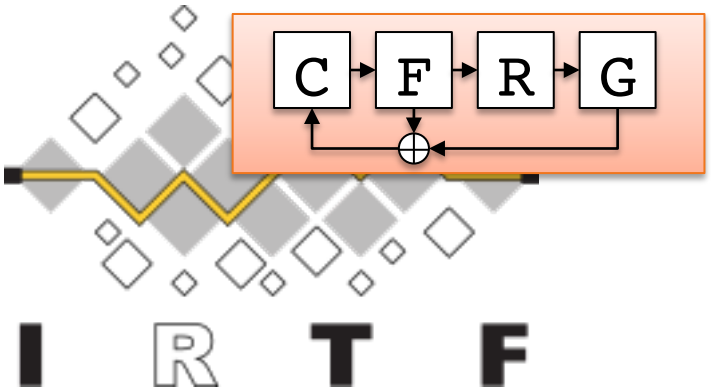


Objective:

make this work!

IETF/IRTFCFRG (Acronym Soup)

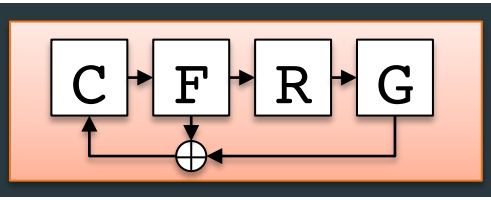




Objective:

make this work!

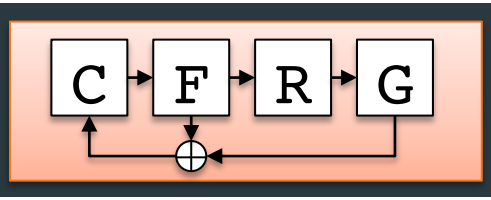
CFRG Charter



The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.

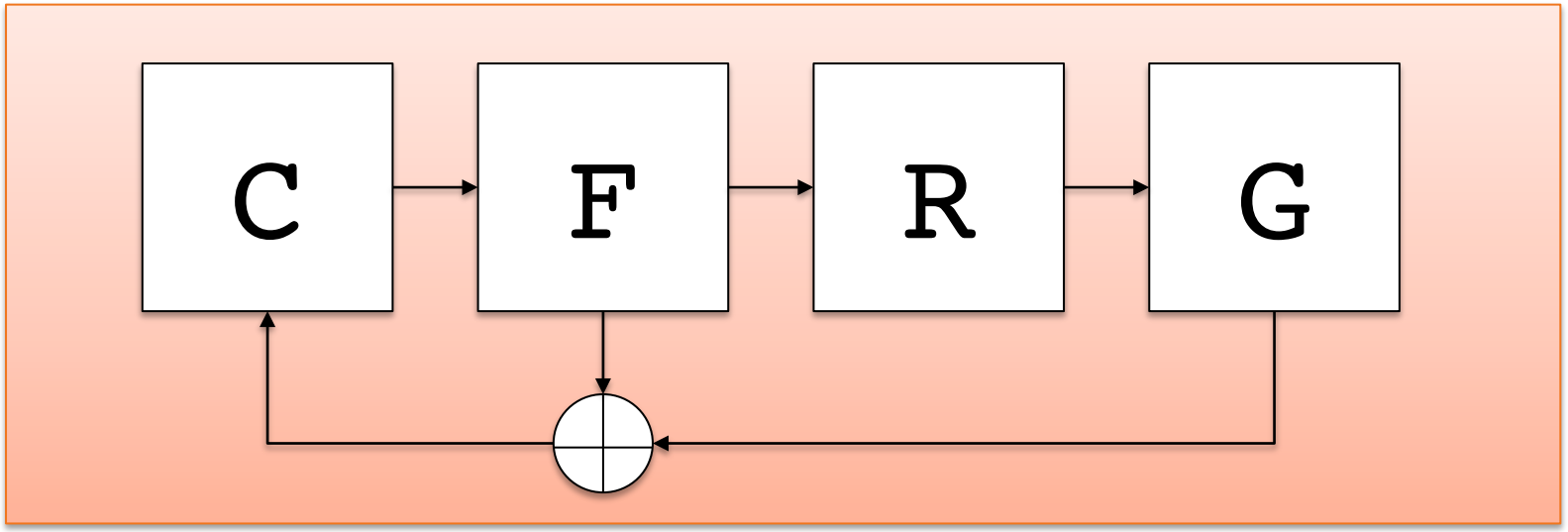
Our goal is to provide a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the use of emerging mechanisms and new uses of existing mechanisms.

How to Get Involved

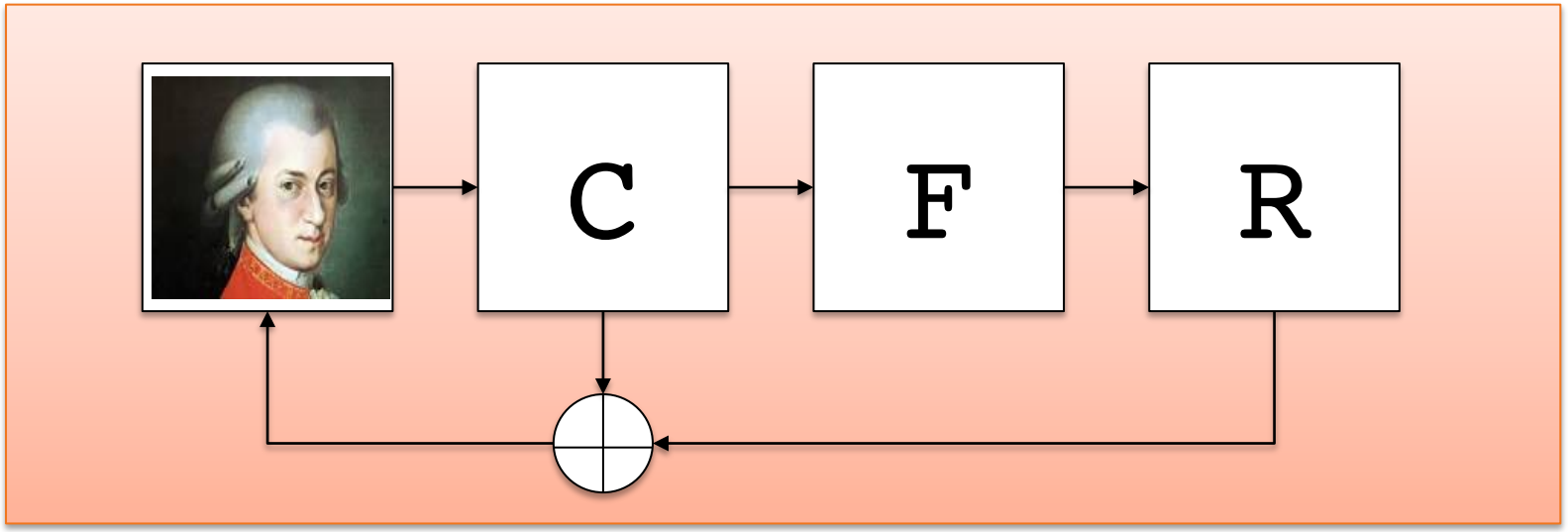


- CFRG needs your help.
- **CFRG is meeting this Thursday 13:30 – 15:30 in the Saulenhalle (first floor of this building).**
    - **Presentations and discussions on memory-hard functions for password hashing, AES-GCM-SIV, hash-based signatures.**
- The meeting is open to everyone.
- Come along on Thursday and find out more.
- AMA.

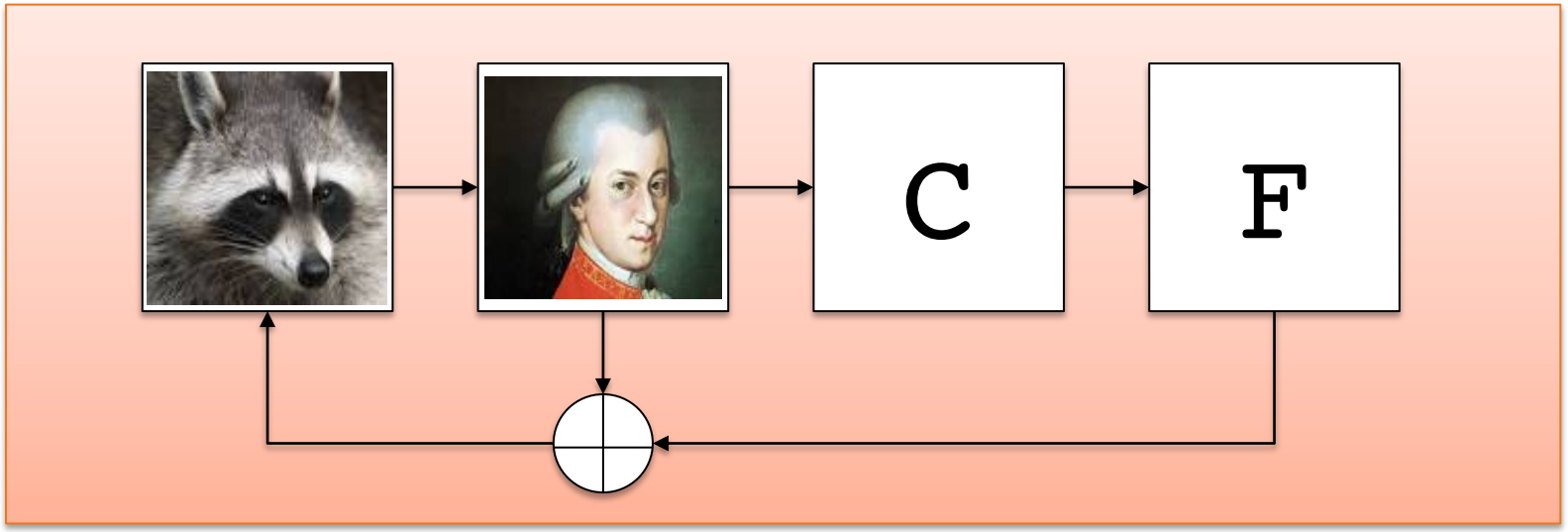
Thanks/Danke/Merci



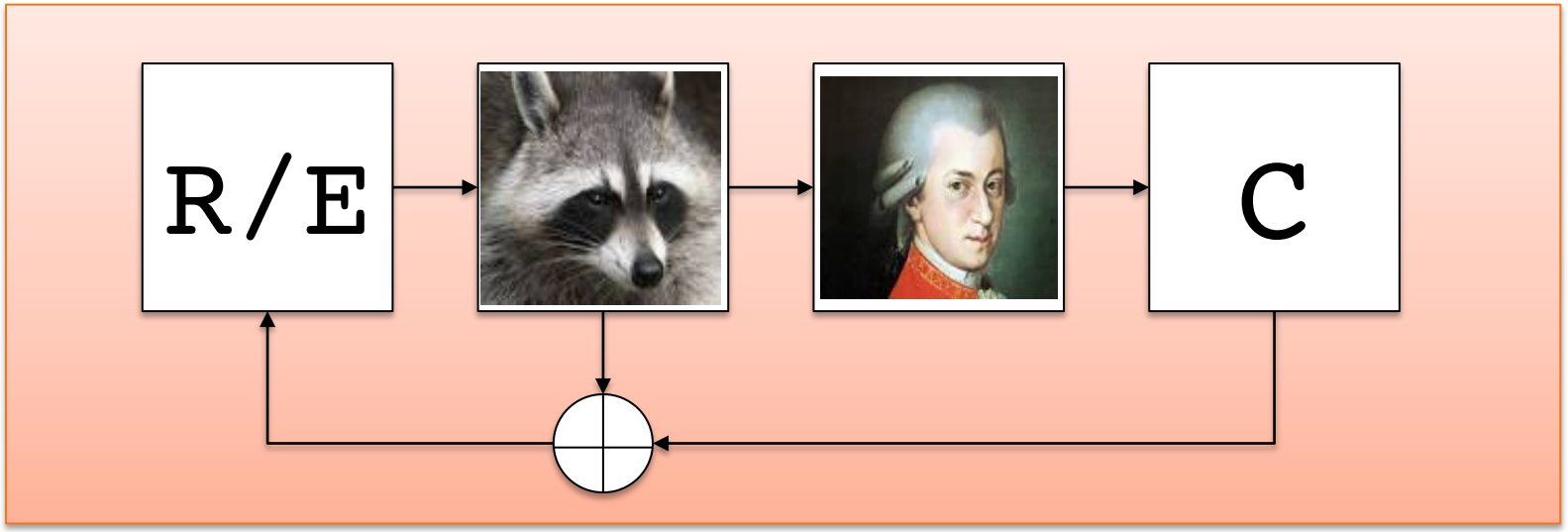
Thanks/Danke/Merci



Thanks/Danke/Merci



Thanks/Danke/Merci



Thanks/Danke/Merci