Is Coordination needed? Round 1

k = 2: 5 honest, 2 byzantine generals

A: Attack

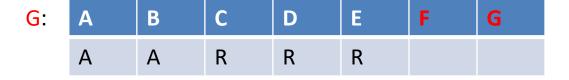
B: Attack

C: Retreat

D: Retreat

E: Retreat

F:	A	В	С	D	Е	F	G
	Α	Α	R	R	R		



Round 2

A,B	Α	В	С	D	E	F	G	Res.
Α	Α	Α	Α	Α	Α	Α	Α	Α
В	Α	Α	Α	Α	Α	Α	Α	Α
С	R	R	R	R	R	Α	Α	R
D	R	R	R	R	R	Α	Α	R
E	R	R	R	R	R	Α	Α	R
F	Α	Α	R	R	R	Α	Α	Α
G	Α	Α	R	R	R	Α	Α	Α
C,D,E	A	В	С	D	E	F	G	Res
Α	А	Α	Α	Α	Α	R	R	Α
В	А	Α	Α	Α	Α	R	R	Α
С	R	R	R	R	R	R	R	R
D	R	R	R	R	R	R	R	R
Е	R	R	R	R	R	R	R	R
F	Α	Α	R	R	R	R	R	R

Conclusion

- 2 byzantine generals can break the algorithm with 5 honest generals
- Both byz. generals send the same messages to the other generals
 - Byzantine generals don't need to coordinate but need to know the number of byzantine generals

Improved Algorithm: Round 1

k = 2: 5 honest, 2 byzantine generals

A: Attack

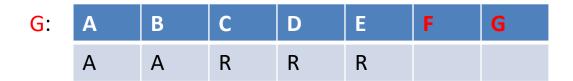
B: Attack

C: Retreat

D: Retreat

E: Retreat

F:	A	В	С	D	Е	F	G
	Α	Α	R	R	R		



Round 2

A,B	Α	В	С	D	Е	F	G
A	Α	Α	Α	Α	Α	Α	Α
В	Α	Α	Α	Α	Α	Α	Α
С	R	R	R	R	R	Α	Α
D	R	R	R	R	R	Α	Α
Е	R	R	R	R	R	Α	Α
F	Α	Α	R	R	R	Α	Α
G	Α	Α	R	R	R	Α	Α
C,D,E	Α	В	С	D	E	F	G
C,D,E	A A	B	C	D A	E A	F R	G R
Α	Α	А	А	А	А	R	R
A B	A A	A A	A A	A A	A A	R R	R R
A B C	A A R	A A R	A A R	A A R	A A R	R R R	R R R
A B C D	A A R R	A A R R	A A R R	A A R R	A A R R	R R R R	R R R R

Round 3

- Every general sends all received vectors to all other generals
 - Vectors which are the same at 2k + 1 generals are from honest generals
 - Vectors which are different at > k generals are from byzantine generals
 - Vectors from byzantine generals will be ignored

Round 3

Every general receives:

A,B	Α	В	С	D	Е	F	G	Res.
A	Α	Α	Α	Α	Α	Α	Α	Α
В	Α	Α	Α	Α	Α	Α	Α	Α
С	R	R	R	R	R	Α	А	R
D	R	R	R	R	R	Α	Α	R
E	R	R	R	R	R	Α	А	R
F	А	Α	R	R	R	Α	А	
G	А	А	R	R	R	А	Α	

->	Re	tre	eat
----	----	-----	-----

C,D,E	Α	В	С	D	Е	F	G	Res.
A	Α	Α	Α	Α	Α	R	R	Α
В	Α	Α	Α	Α	Α	R	R	Α
С	R	R	R	R	R	R	R	R
D	R	R	R	R	R	R	R	R
E	R	R	R	R	R	R	R	R
F	А	А	R	R	R	R	R	
G	А	А	R	R	R	R	R	

F,G	Α	В	С	D	Е	F	G
Α	х	Х	Х	x	X	Х	X
В	х	x	x	x	X	x	X
С	х	x	x	x	X	x	X
D	х	X	X	X	X	X	X
Ε	х	Х	Х	x	Х	Х	X
F	х	Х	Х	Х	X	X	X
G	X	X	X	X	X	X	X