Boolean functions in Cryptography

Nikolay S. Kaleyski
PhD Student, Selmer Center, UiB

What is a (vectorial) Boolean function?

An (n, m)-function maps sequences of n bits to sequences of m bits

f(0000) = 00
f(1011) = 10
f(1111) = 00

(4,2)-function

x	f(x)	x	f(x)
0000	00	1000	10
0001	01	1001	11
0010	01	1010	11
0011	00	1011	10
0100	10	1100	00
0101	11	1101	01
0110	11	1110	01
0111	10	1111	00

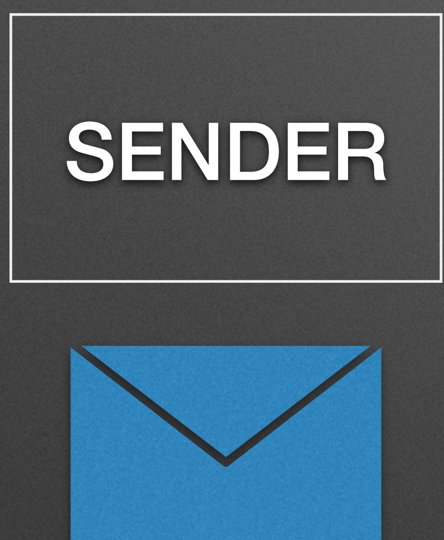
What is it good for?

- Propositional logic and artificial intelligence
- Electrical and computer engineering (circuits)
- Game theory
- Combinatorics
- Integer programming
- *Cryptography*
- …

Information security and Cryptography

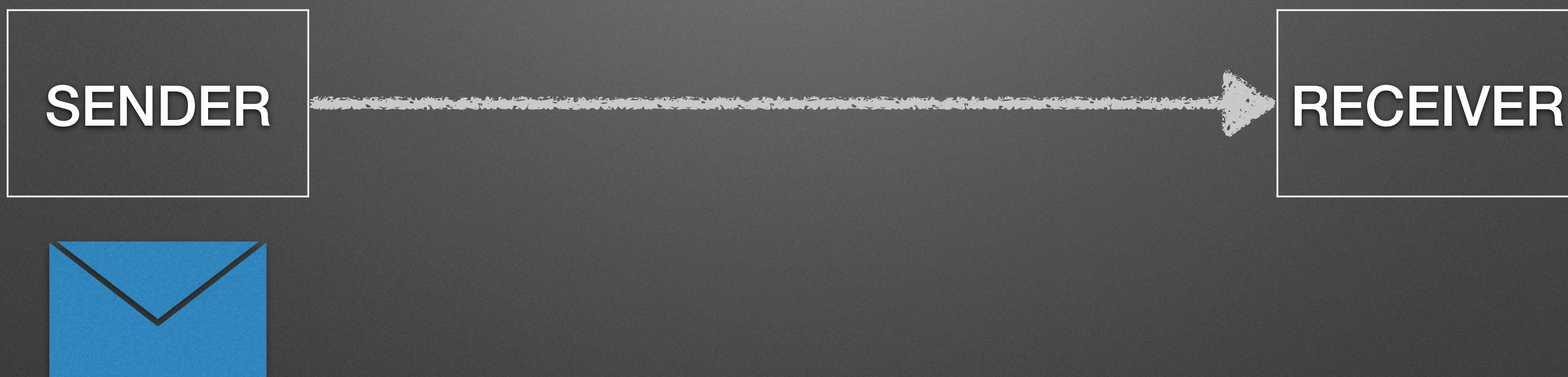
SENDER

Information security and Cryptography



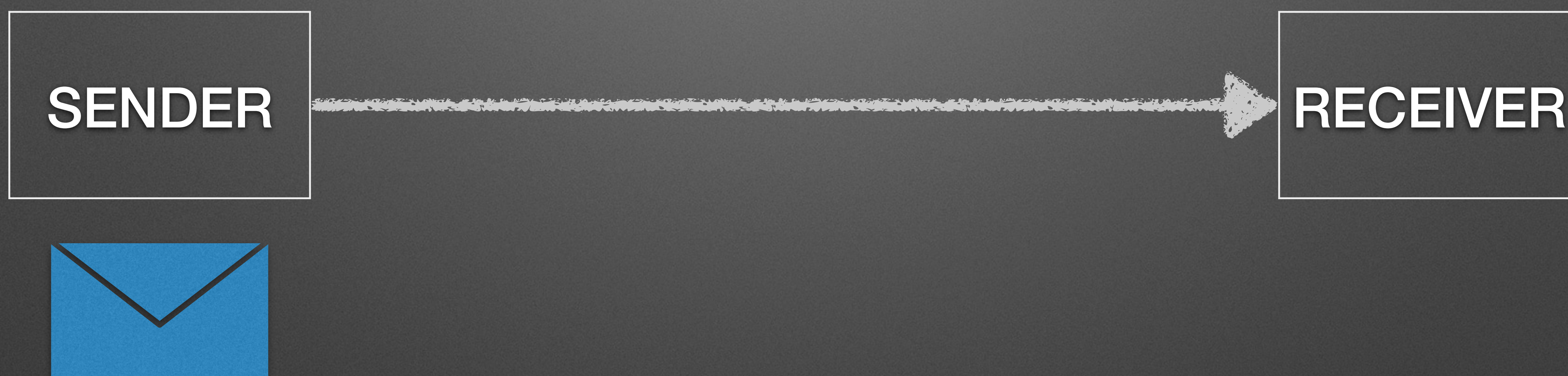
Information security and Cryptography

Information security and Cryptography

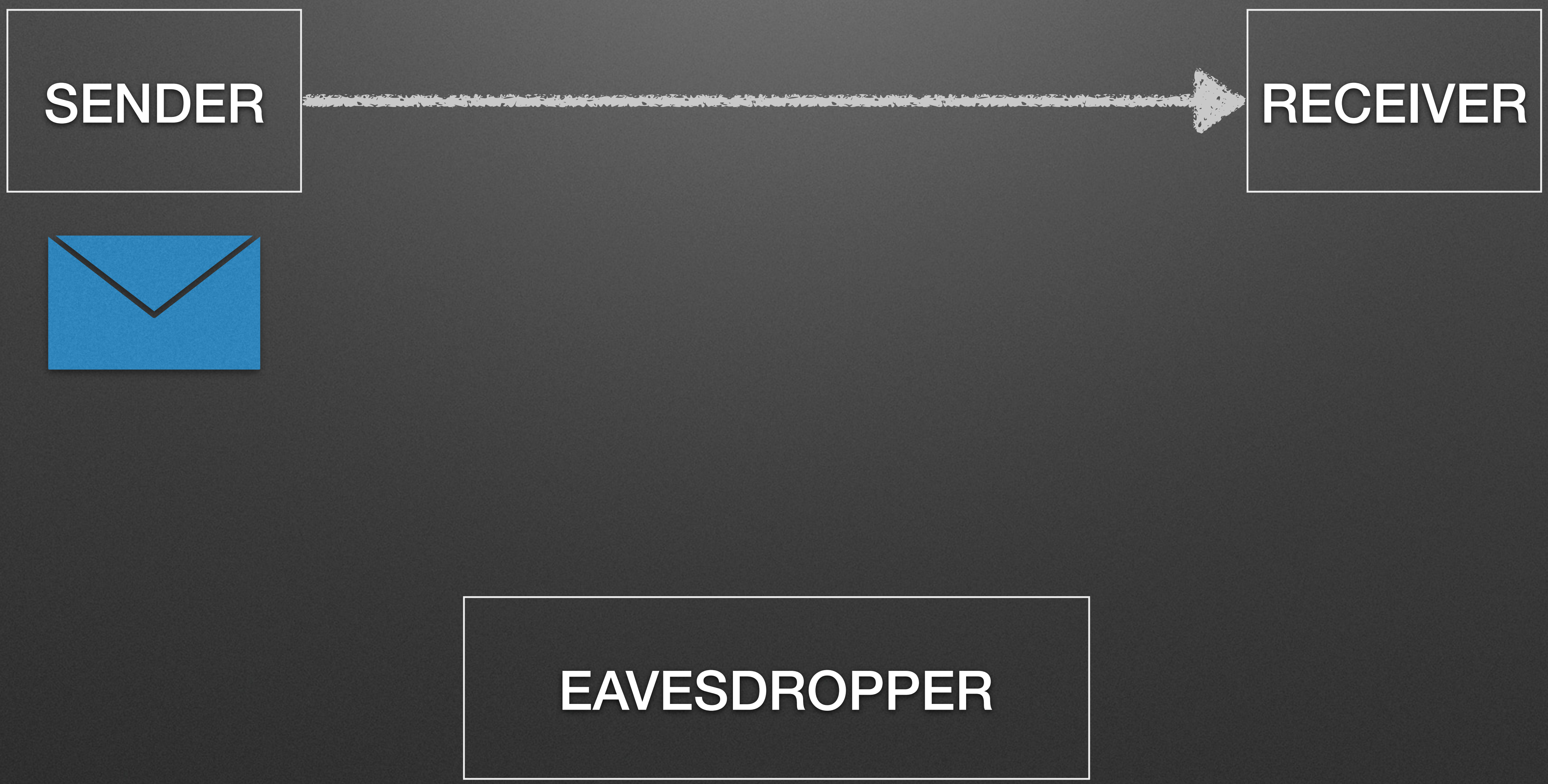


Information security and Cryptography

Information security and Cryptography



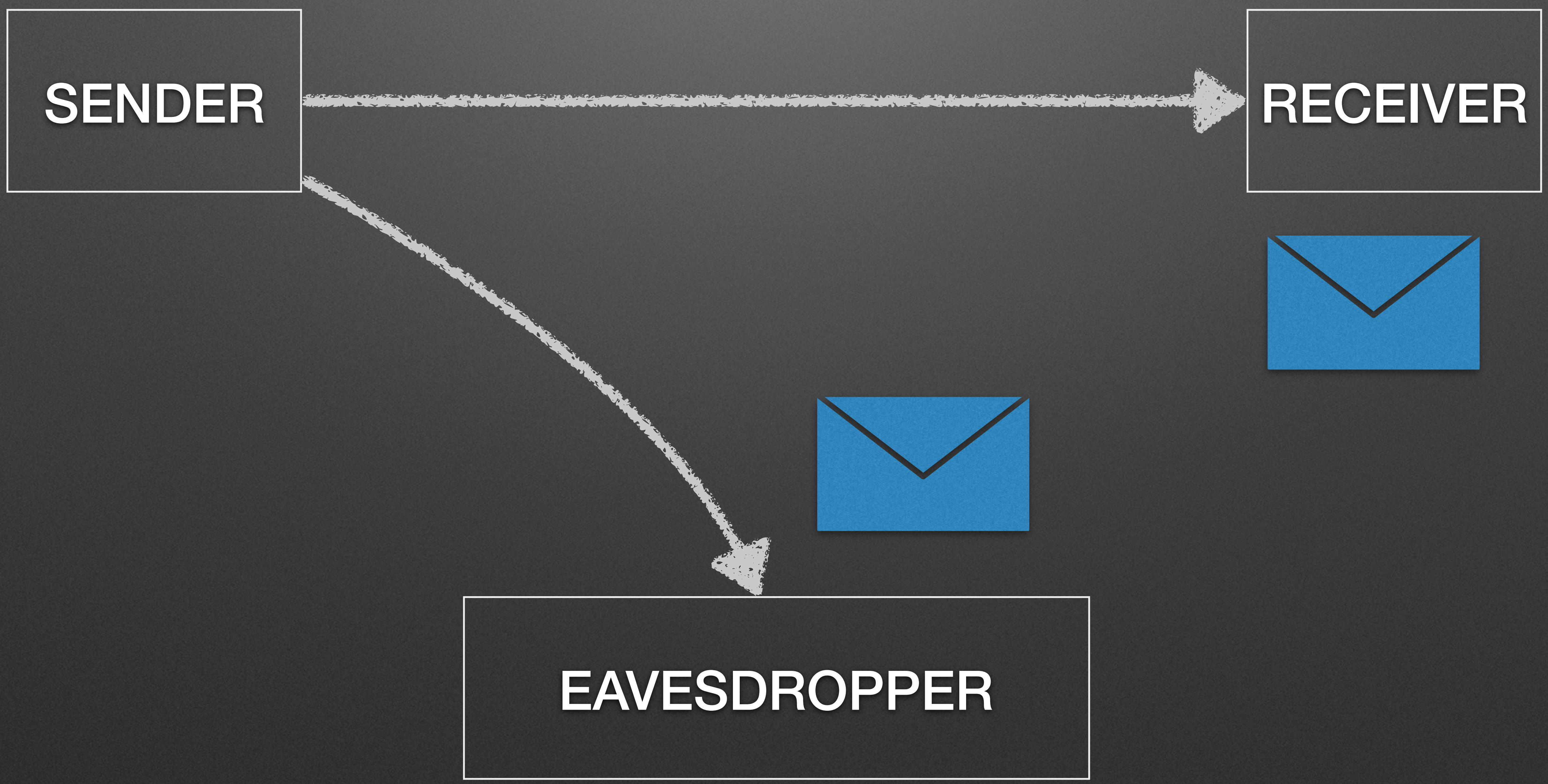
Information security and Cryptography



Information security and Cryptography

Information security and Cryptography

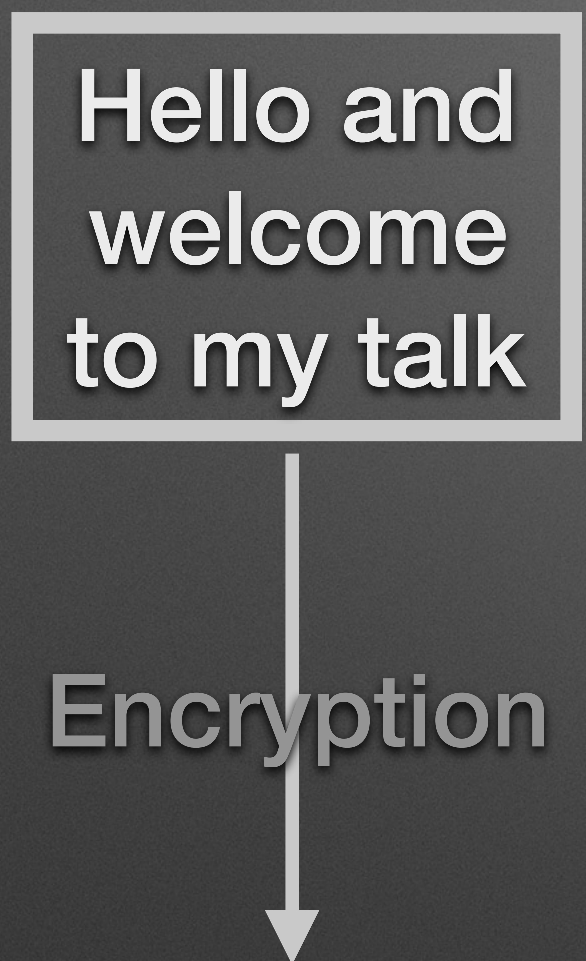
Information security and Cryptography



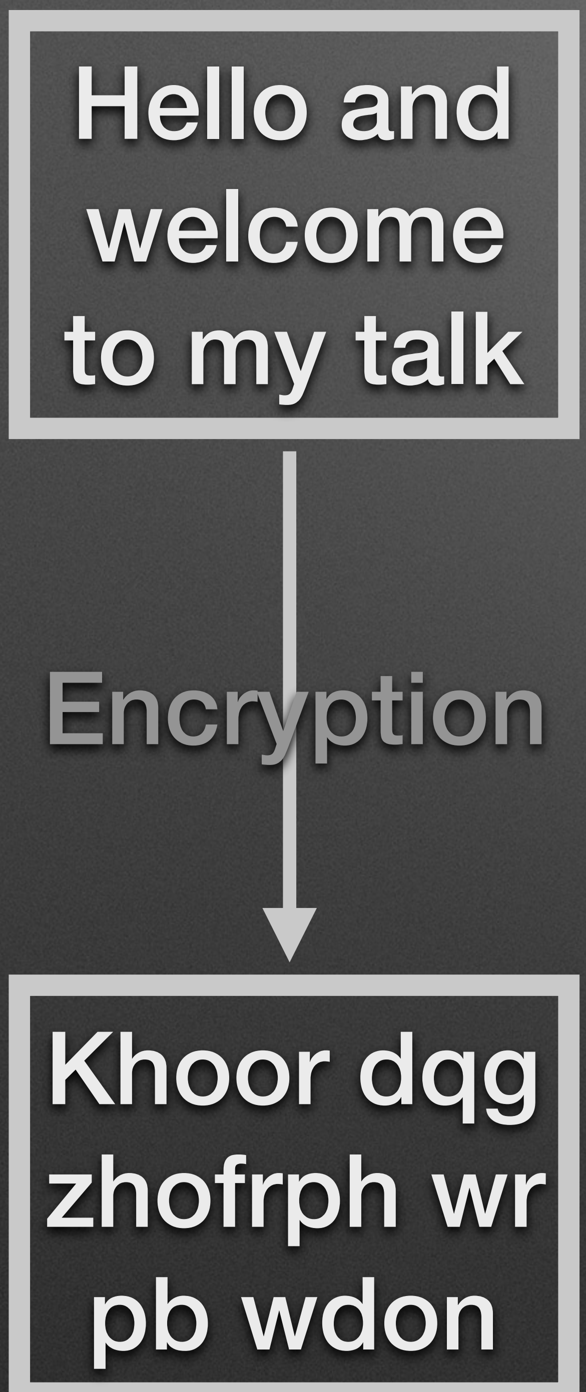
Encryption/Decryption

Hello and welcome to my talk

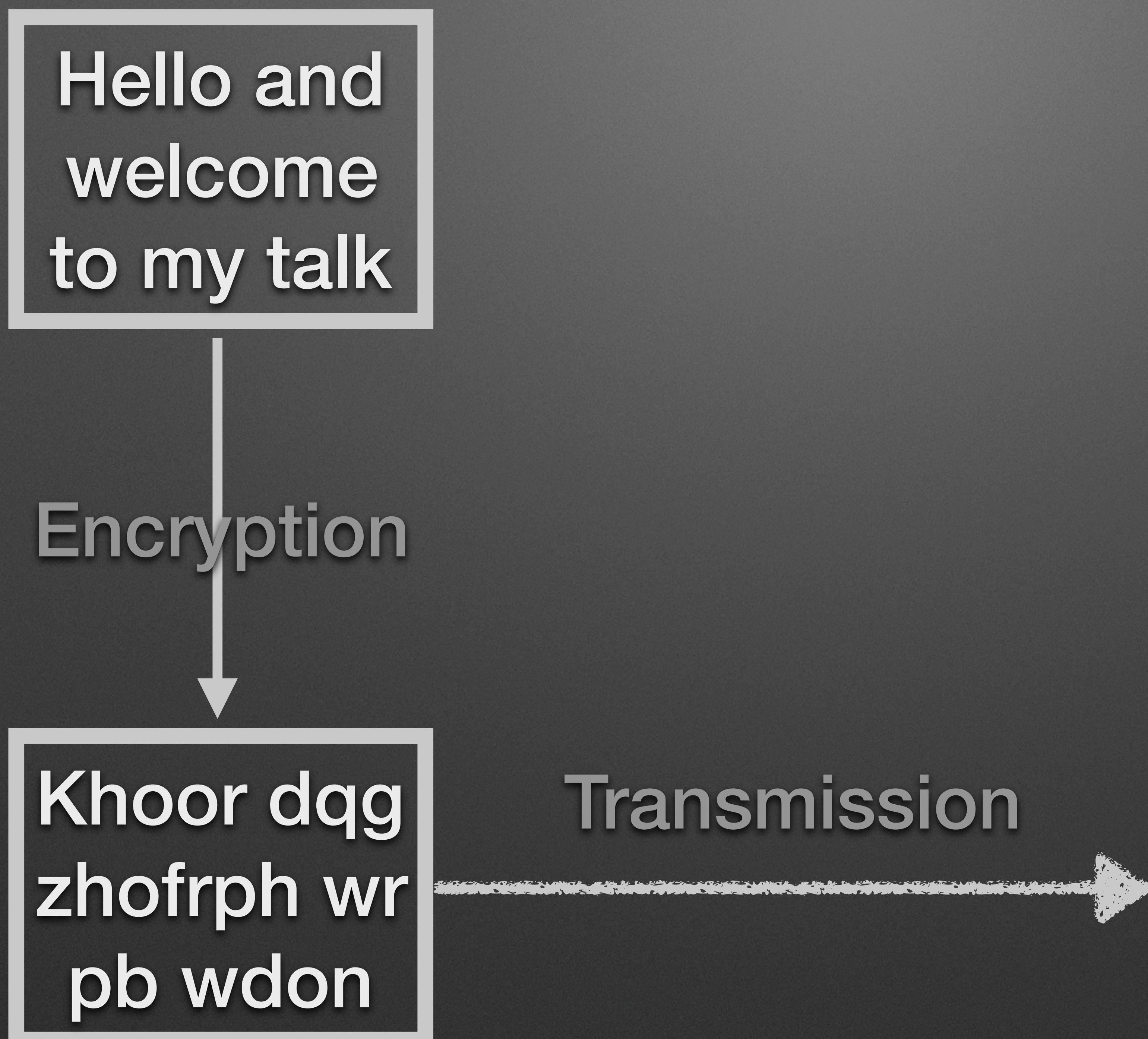
Encryption/Decryption



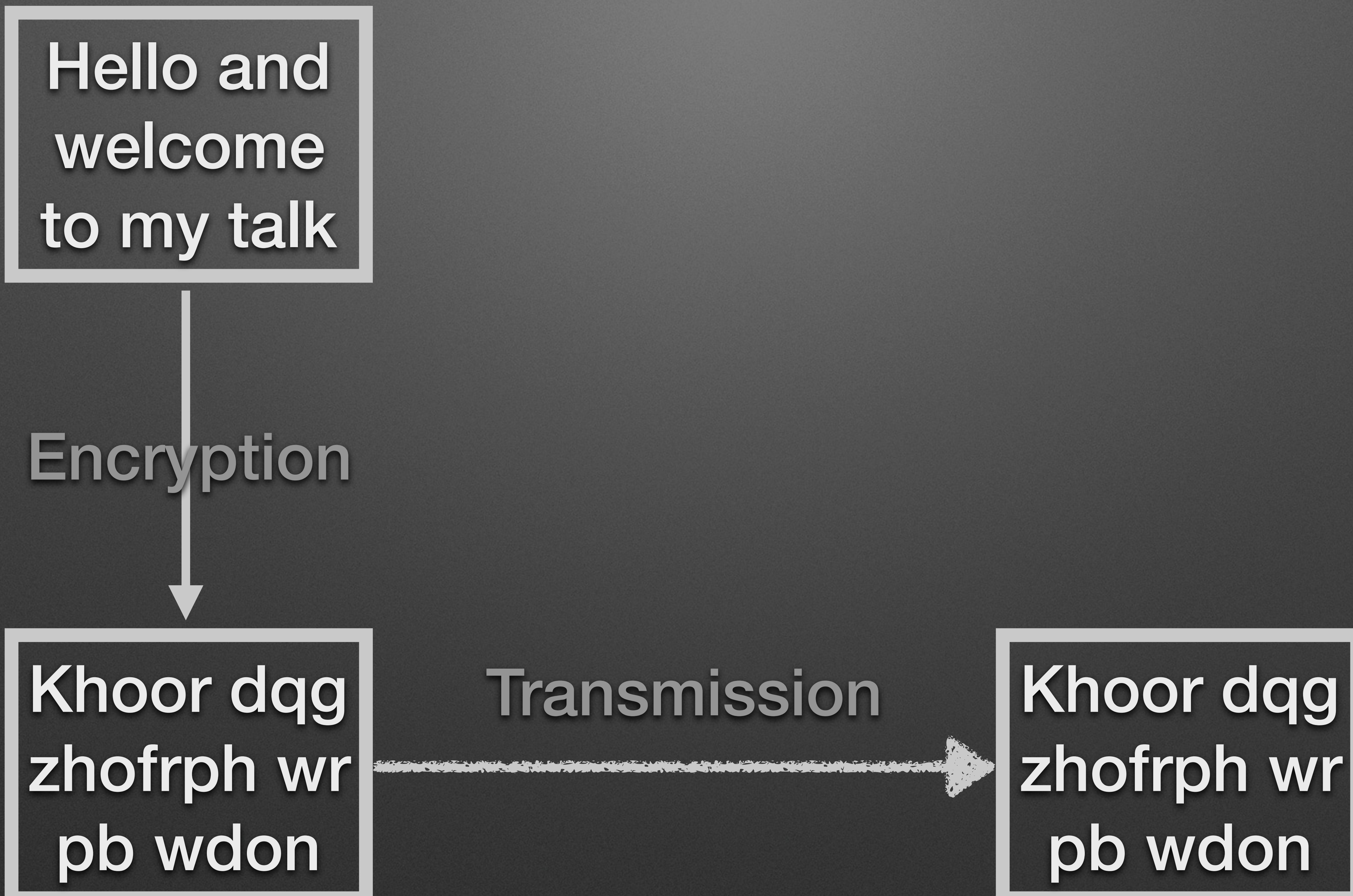
Encryption/Decryption



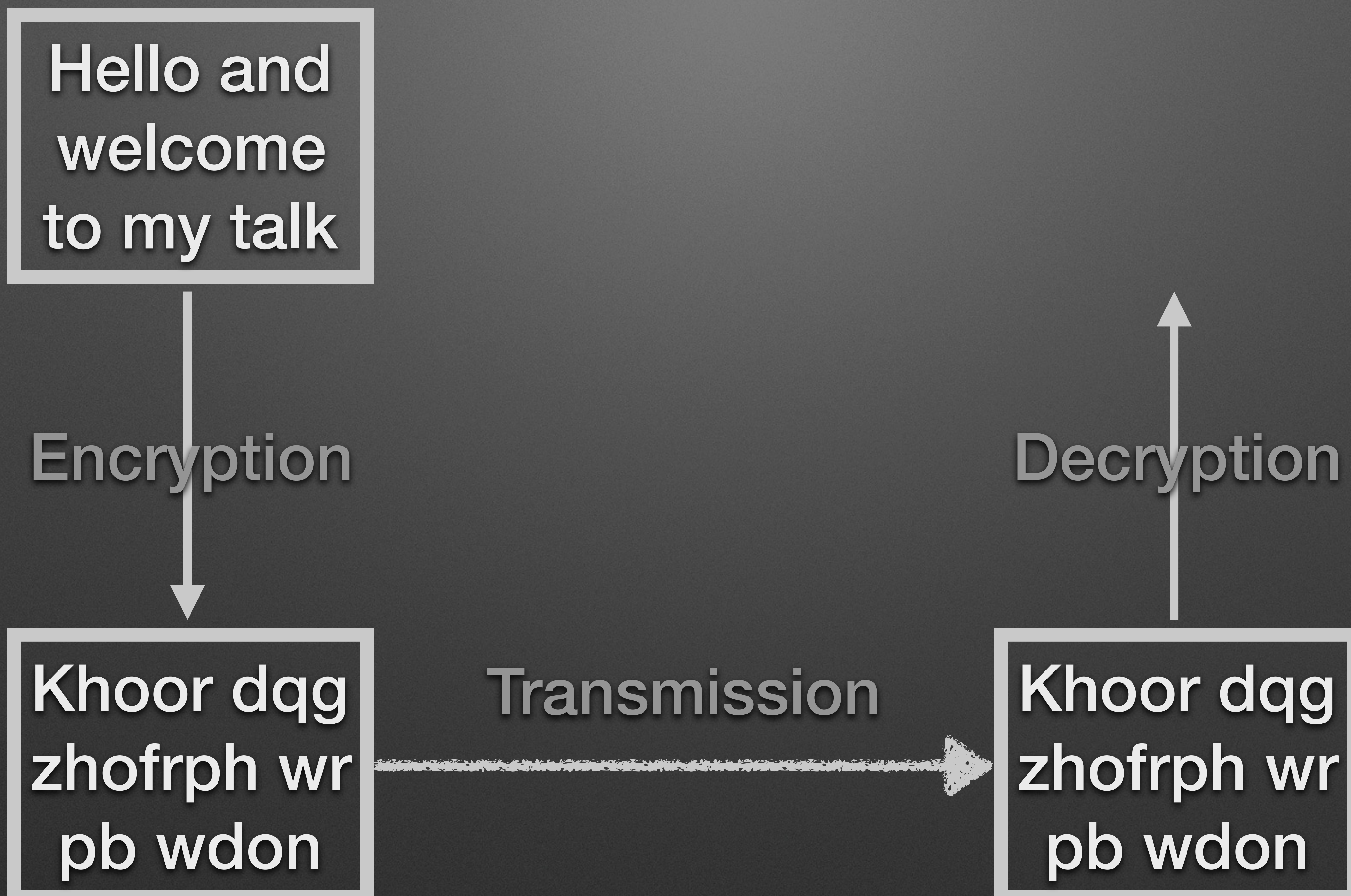
Encryption/Decryption



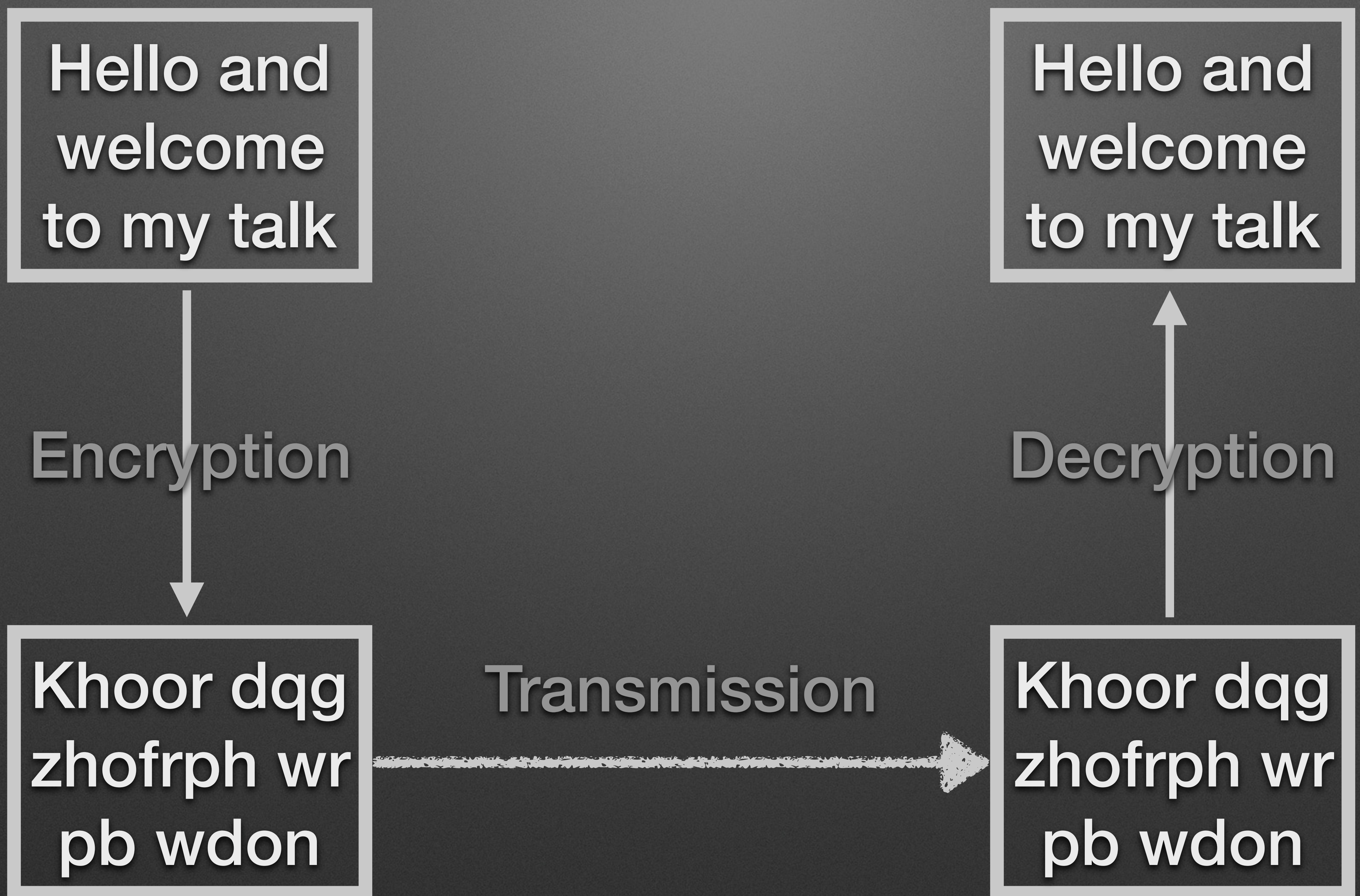
Encryption/Decryption



Encryption/Decryption



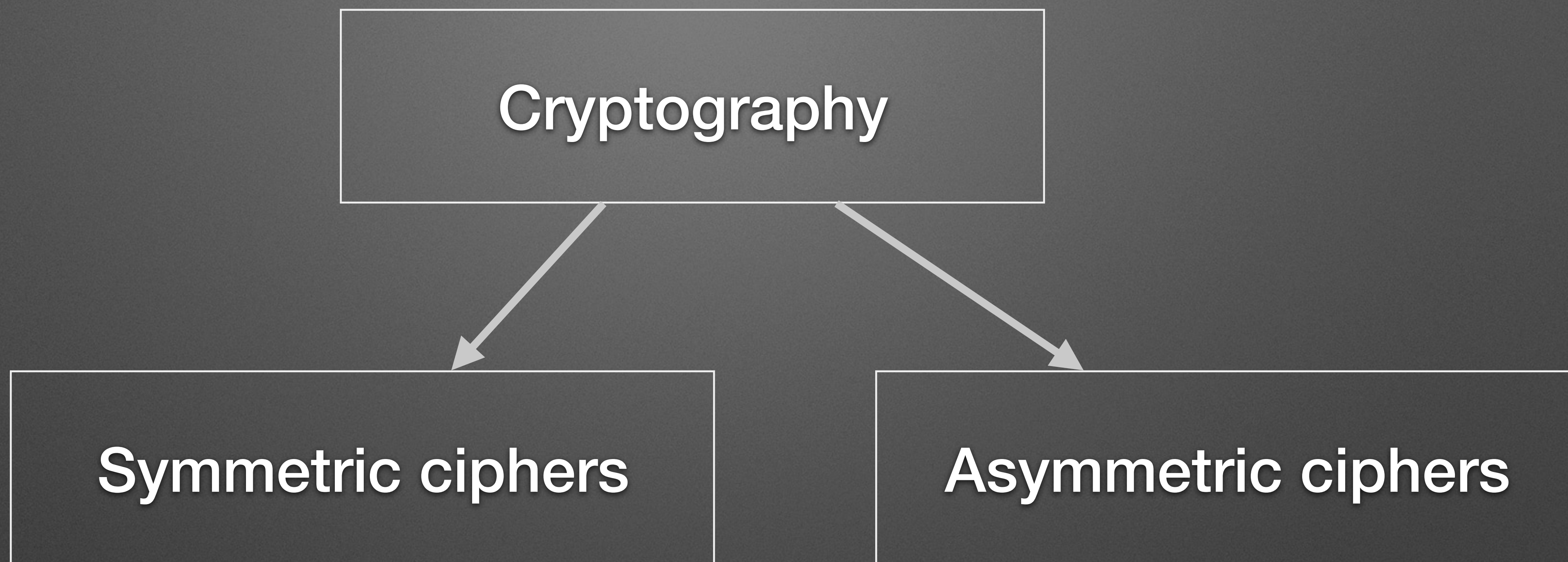
Encryption/Decryption



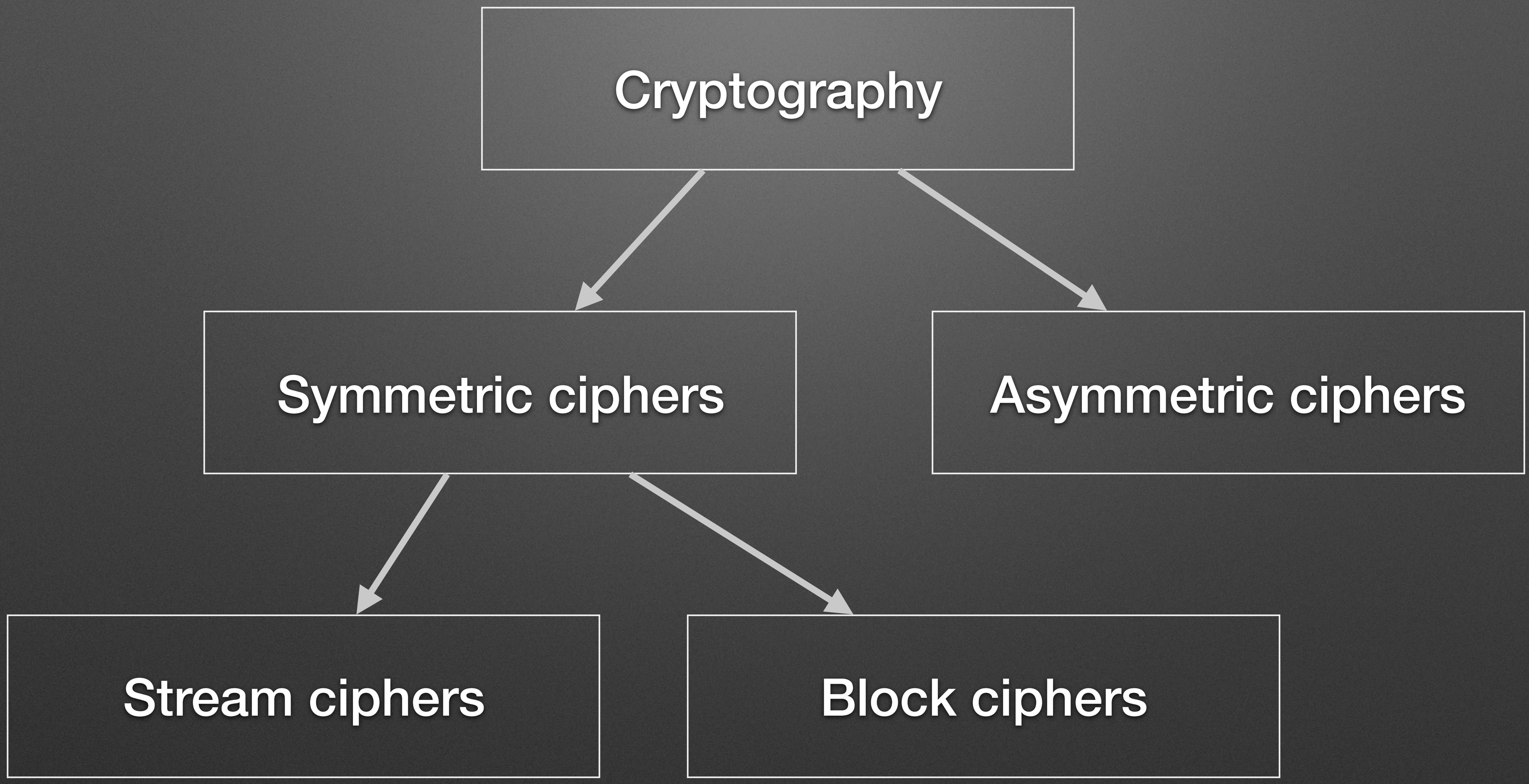
Modern Cryptography

Cryptography

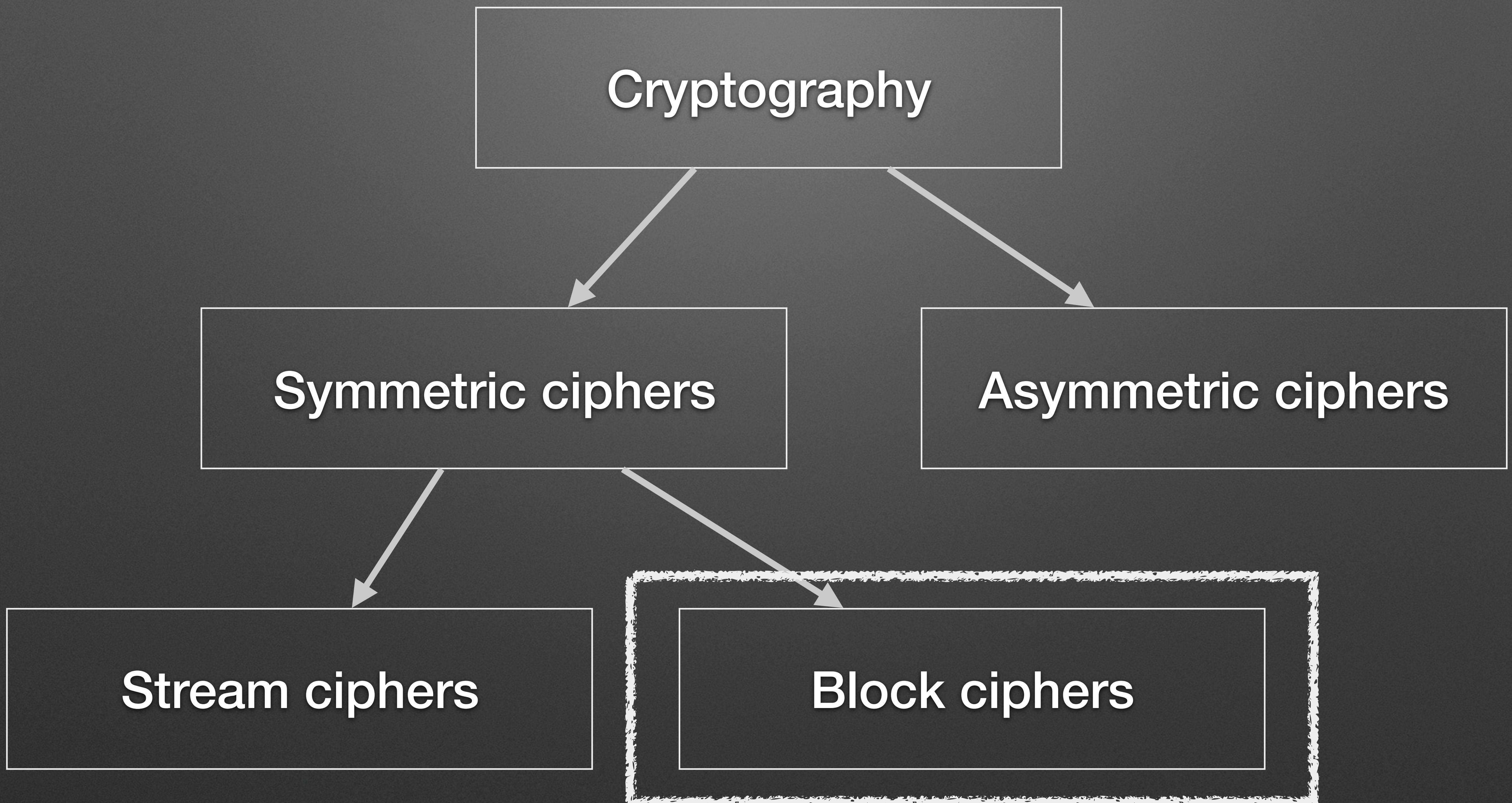
Modern Cryptography



Modern Cryptography



Modern Cryptography

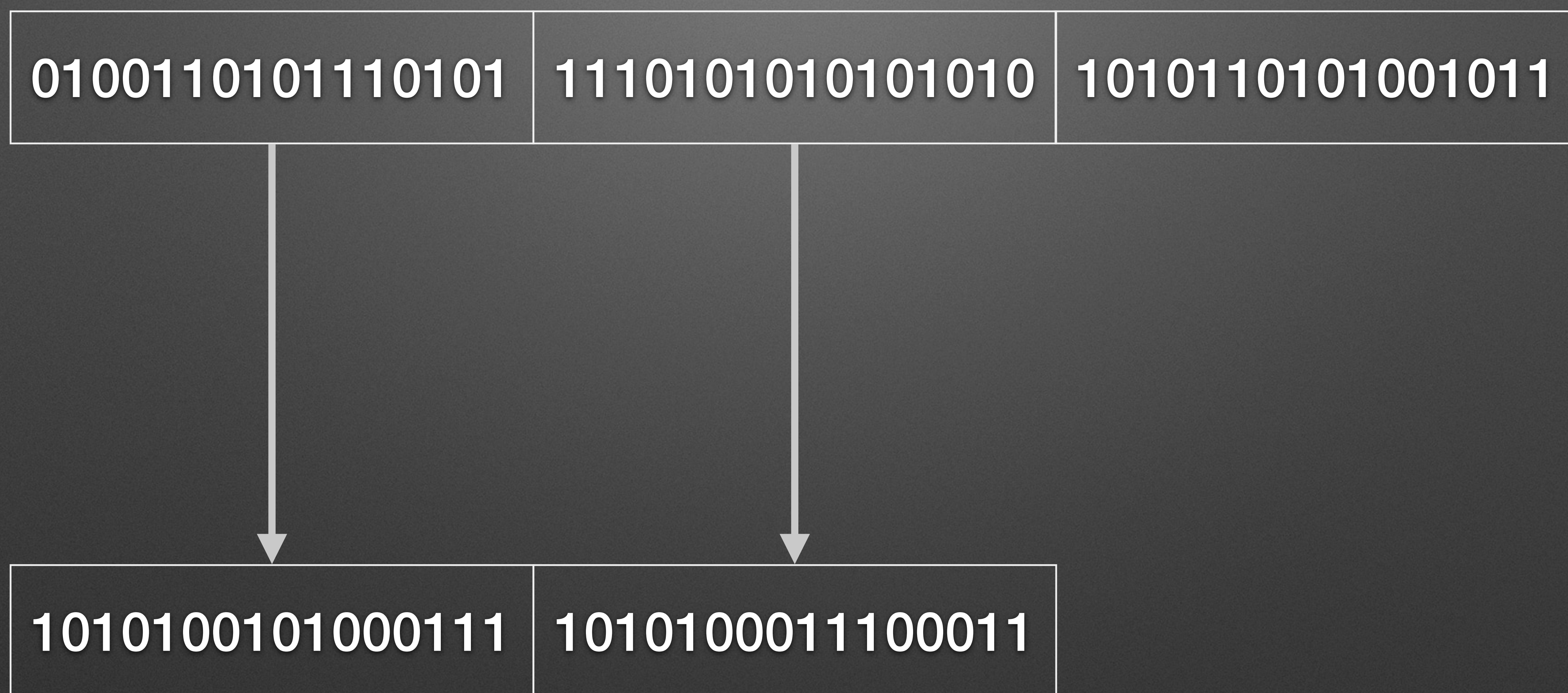


Block ciphers

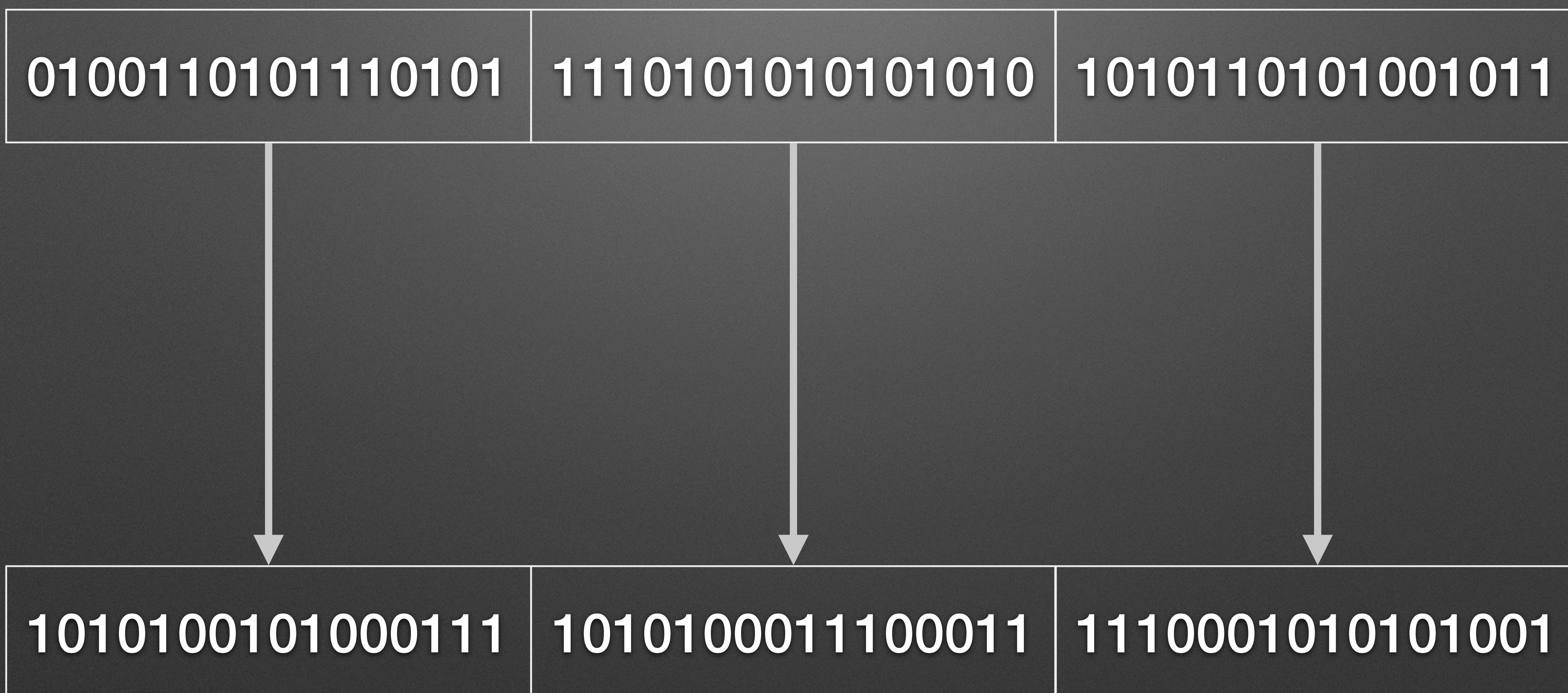
0100110101110101	1110101010101010	1010110101001011

Block ciphers

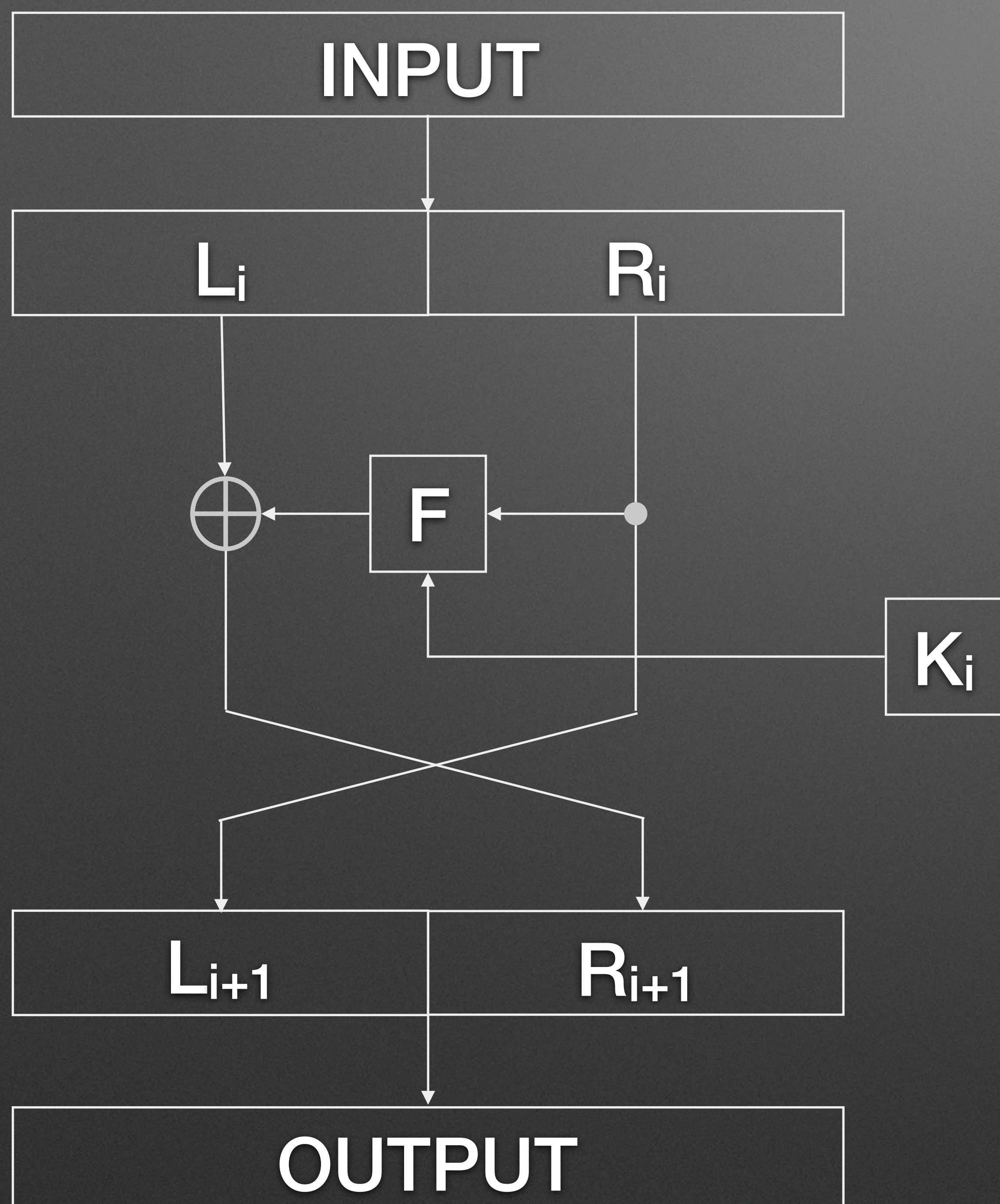
Block ciphers



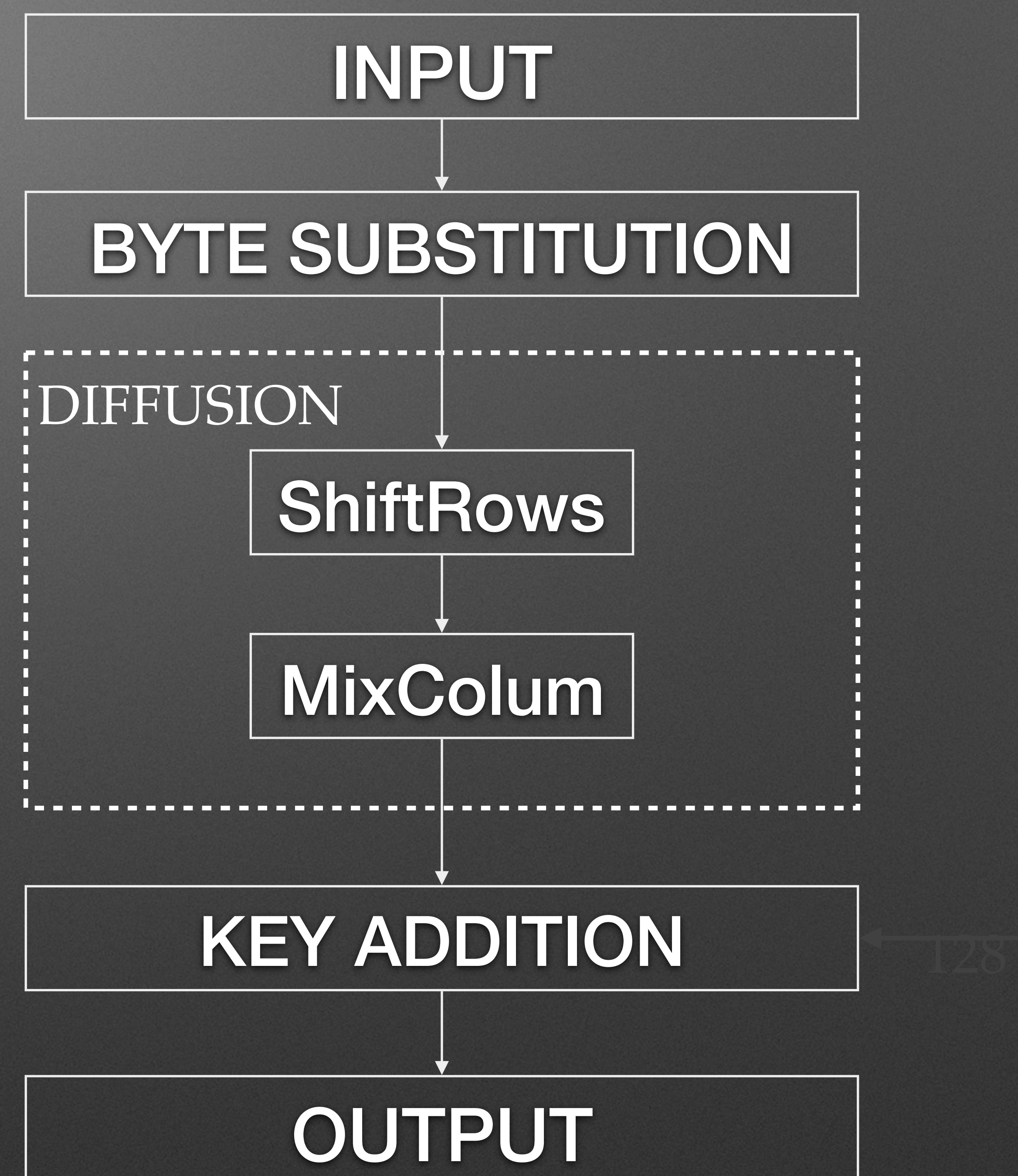
Block ciphers



How to make block ciphers

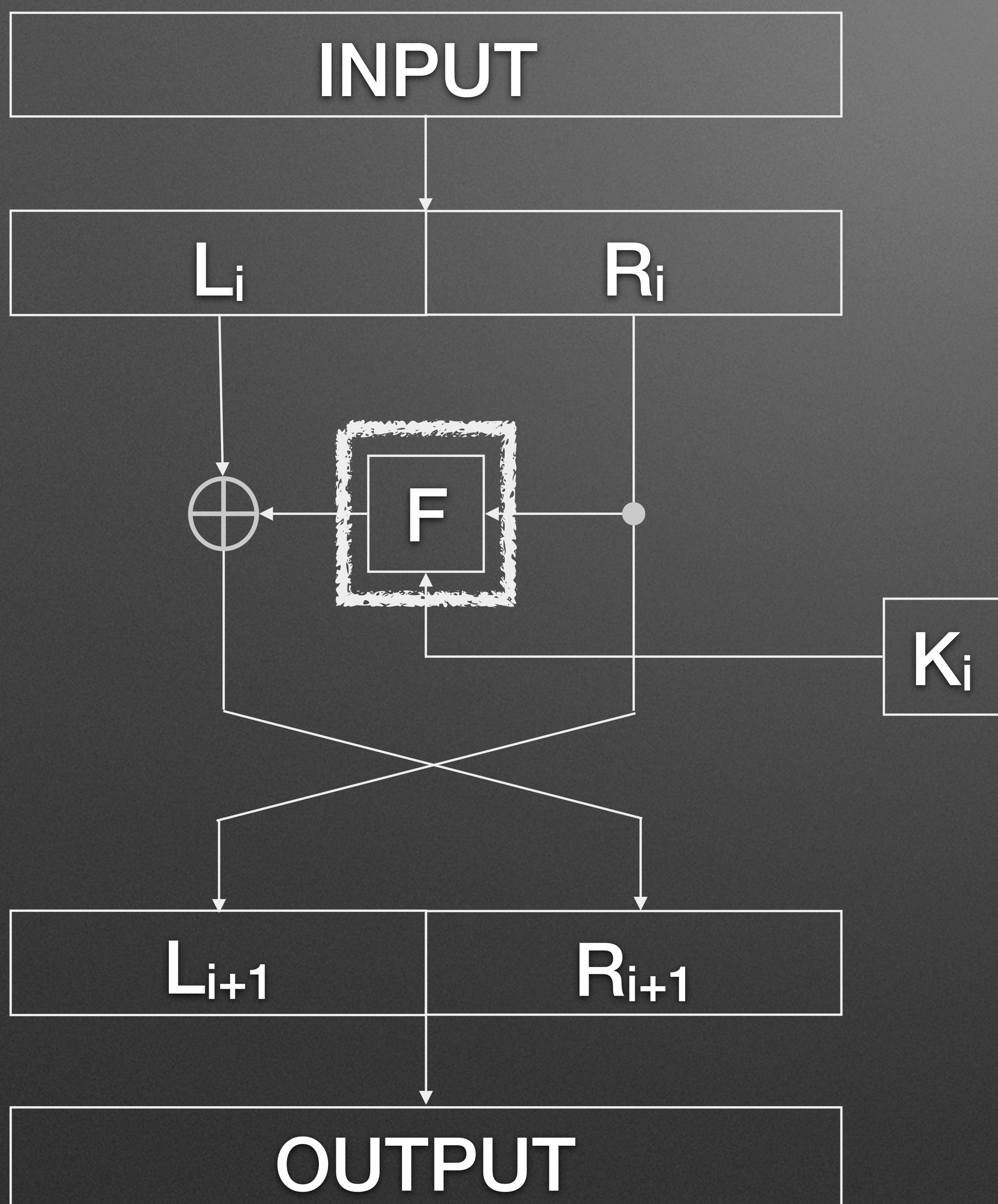


Feistel Network

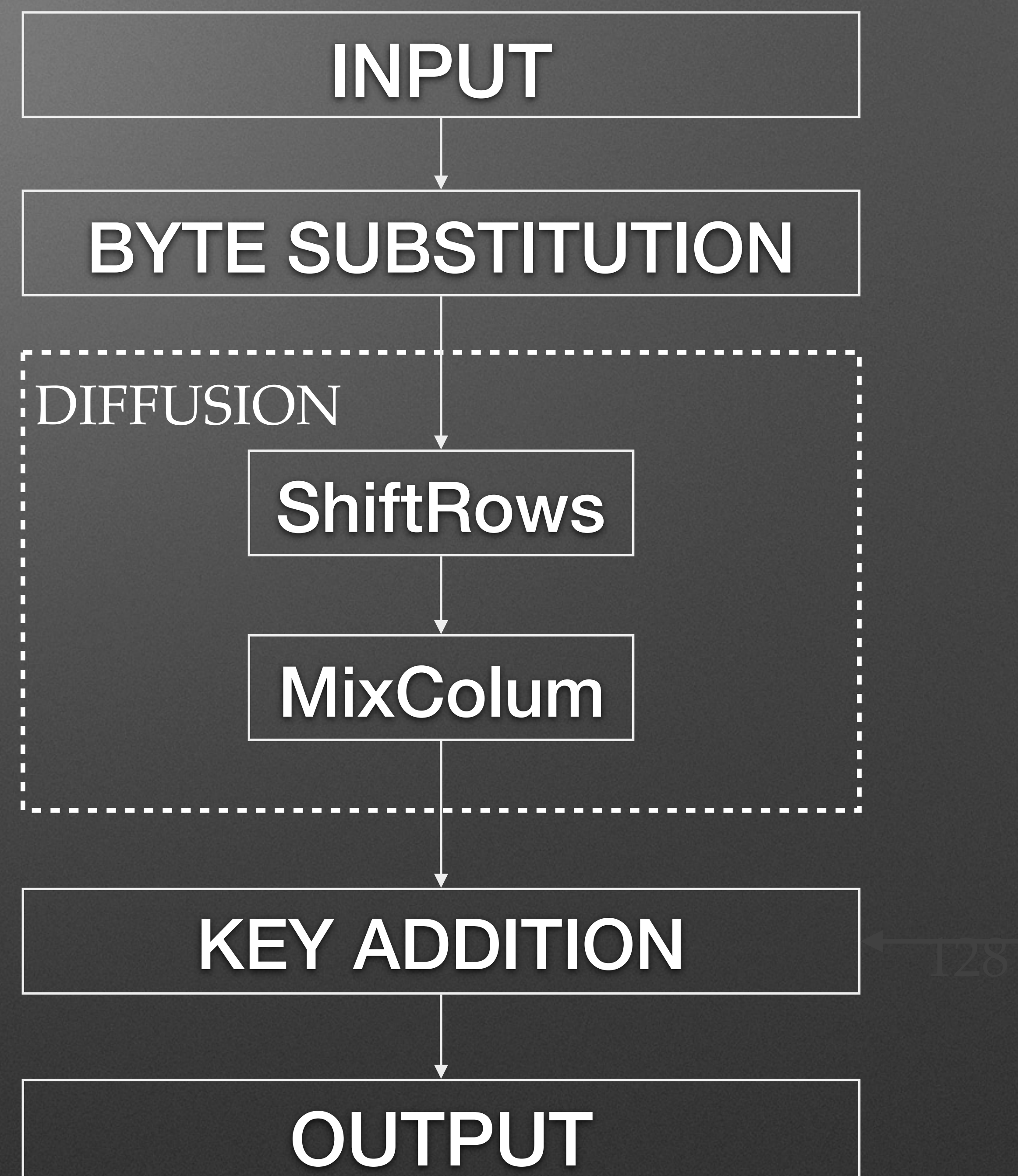


AES round structure

How to make block ciphers

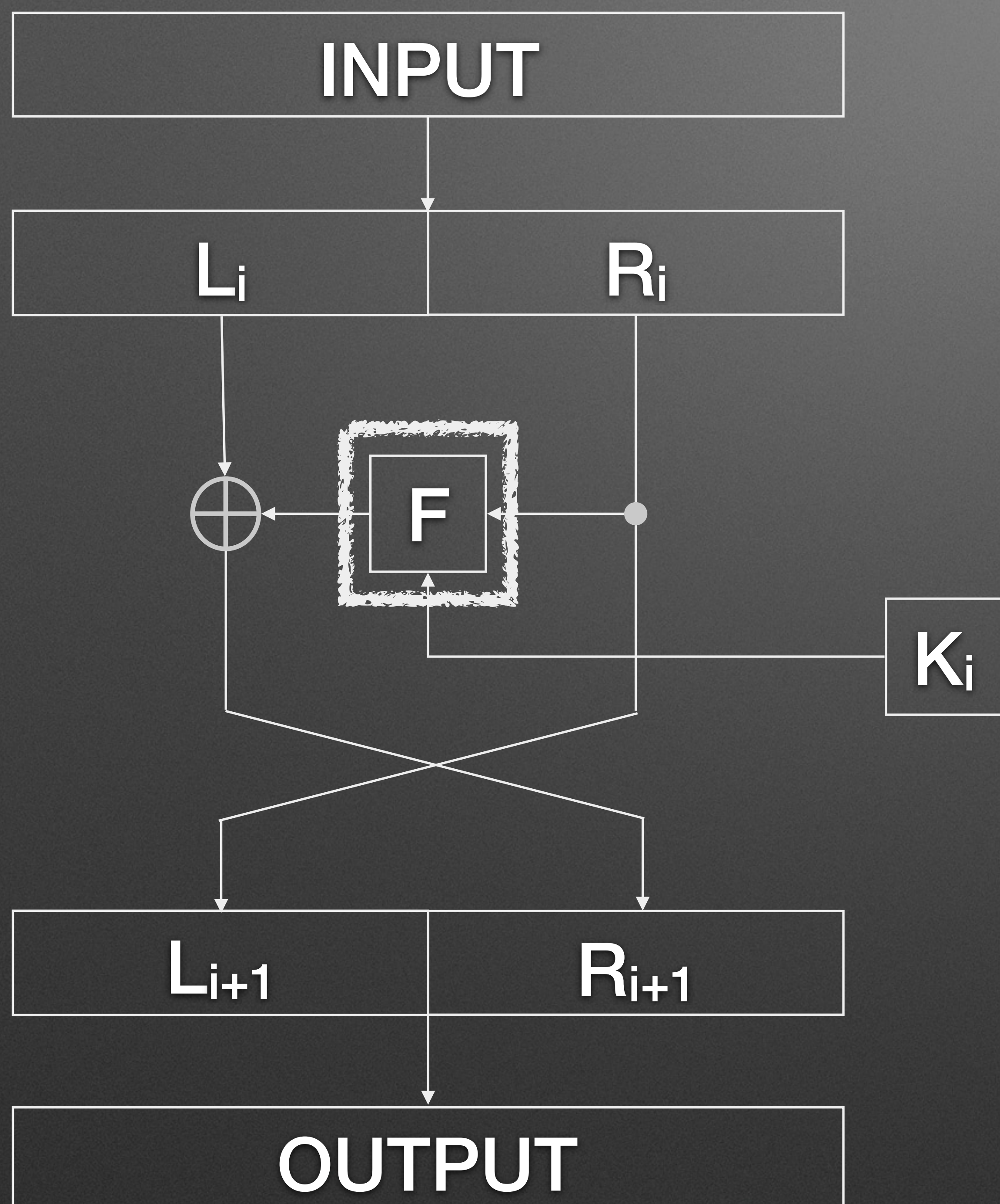


Feistel Network

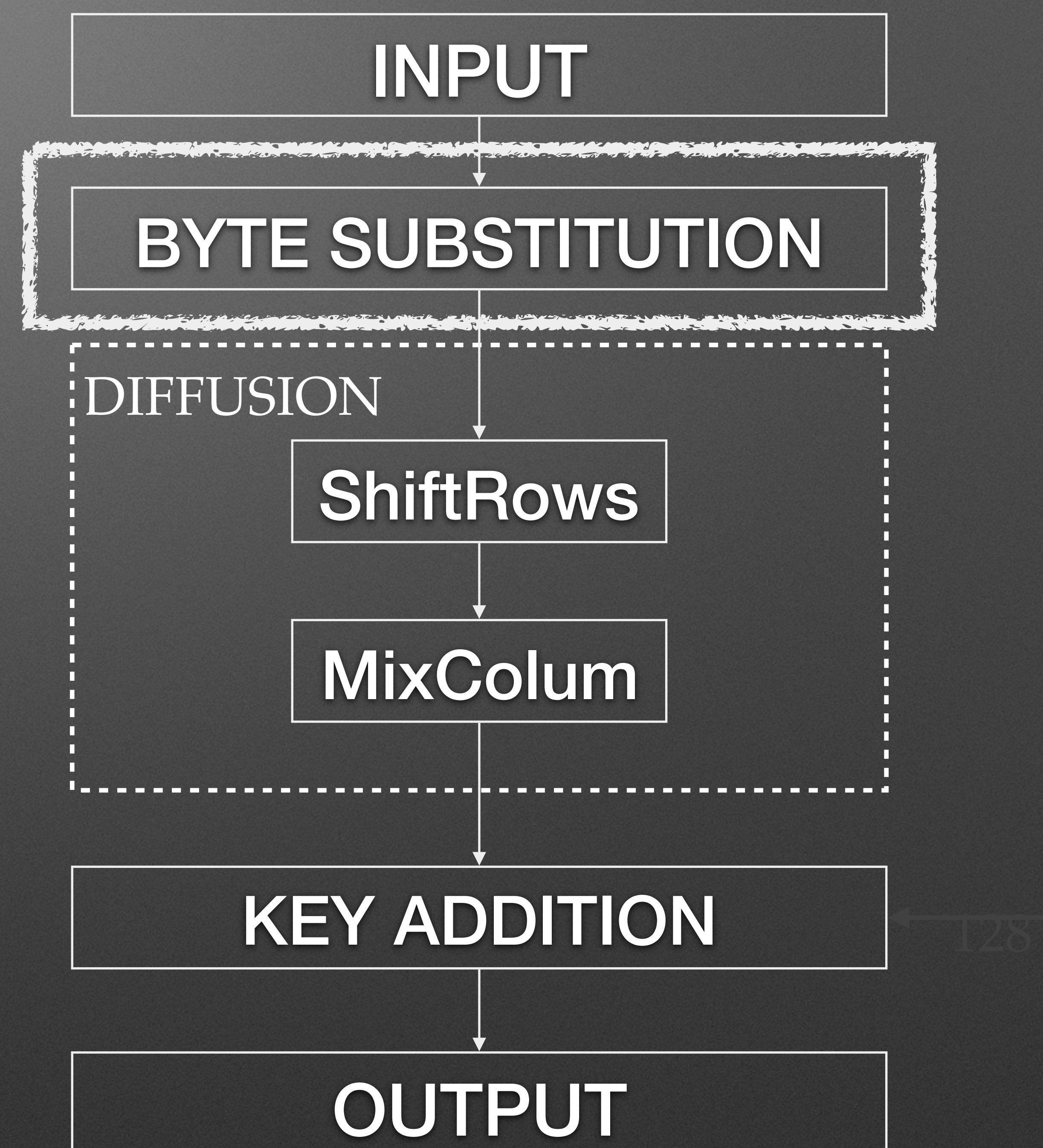


AES round structure

How to make block ciphers



Feistel Network



AES round structure

A good (8,8)-function

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
4	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

01011100 = 5C

↓

01001010 = 4A

A good (8,8)-function

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
4	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	8
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

01011100 = 5C

↓

01001010 = 4A

But why?

Attacks and countermeasures

Differential Cryptanalysis

Linear Cryptanalysis

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis →

Linear Cryptanalysis

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

Linear Cryptanalysis

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis →

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis → Nonlinearity

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis → Nonlinearity

AB Functions

Higher Order
Differential Attacks

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis → Nonlinearity

AB Functions

Higher Order Differential Attacks →

Attacks and countermeasures

Differential Cryptanalysis → Differential uniformity

APN Functions

Linear Cryptanalysis → Nonlinearity

AB Functions

Higher Order Differential Attacks → Algebraic degree

Mathematical representation

- Take n = 8
- There are 256 values that can be expressed with 8 bits
- There are 256 elements in the finite field $\mathbb{F}_{2^8}$
  - These are even typically written as binary vectors, e.g. (0,1,0,0,1,1,0,1)
- Functions $F : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ have a polynomial representation
- The *Gold function* $F(x) = x^3$ has optimal differential uniformity over any finite field $\mathbb{F}_{2^n}$

Research problems

- APN Permutations on an even number of bits:
  - *Not for four bits*
  - *Browning, K. A., Dillon, J. F., McQuistan, M. T., & Wolfe, A. J. (2010). An APN permutation in dimension six. Finite Fields: theory and applications, 518, 33-42.*
  - *Eight, ten, twelve … ???*

- Infinite families of APN functions
  - *APN functions have been known for around 30 years*
  - *There are ca. 16 infinite families of APN functions, e.g.* $F(x) = x^3 + a^{-1}\mathrm{Tr}_n(a^3x^9)$ *over* $\mathbb{F}_{2^n}$
  - *There are over 400 APN functions on 7 bits and over 8000 APN functions on 8 bits*

- Properties of APN functions and APN functions with special properties
  - *Only one known example of an APN function which is not of degree 2*
  - *No known APN function on* n *bits of degree* n *for any* n
  - *…*

Progress at UiB

- Construction of new infinite families of APN functions
  - L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, I. Villa: *Constructing APN functions through isotopic shifts*
  - L. Budaghyan, T. Helleseth, N. S. Kaleyski: *A new family of APN quadrinomials*
  - Both submitted to IEEE Transactions on Information Theory

Progress at UiB

- Properties of APN functions
  - I. Villa: *On APN functions L1(x3)+L2(x9) with linear L1 and L2*, Cryptography and Communications. 10.1007/s12095-018-0283-8
  - N. S. Kaleyski: *Changing APN Functions at Two Points*, Cryptography and Communications. 10.1007/s12095-019-00366-6
  - L. Budaghyan, M. Calderini, I. Villa: *On relations between CCZ- and EA-equivalences*, Cryptography and Communications. 10.1007/s12095-019-00367-5
  - L. Budaghyan, C. Carlet, D. Davidova, T. Helleseth, F. Ihringer, T. Penttila: *Relation between o-equivalence and EA-equivalence for Niho bent functions*, Submitted to Finite Fields and Their Applications
  - M. Calderini, I. Villa: *On the Boomerang Uniformity of some Permutation Polynomials*, Submitted to Cryptography and Communications
  - L. Budaghyan, C. Carlet, T. Helleseth, N. S. Kaleyski: *On the distance between APN functions,* Submitted to IEEE Transactions on Information Theory

Progress at UiB

- Partially APN functions
  - L. Budaghyan, N. S. Kaleyski, S. Kwon, C. Riera, P. Stanica: *Partially APN Boolean functions and classes of functions that are not APN infinitely often*, Cryptography and Communications. 10.1007/s12095-019-00372-8
  - L. Budaghyan, N.S. Kaleyski, C. S. Riera, P. Stanica: *Partially APN functions with APN-like polynomial representations*, Submitted to Designs, Codes and Cryptography

Thank you!