Möjligheternas dag 2024
Årskurs 4-6

Presentationen skapad av
Malin Bernelf, adjunkt i matematik

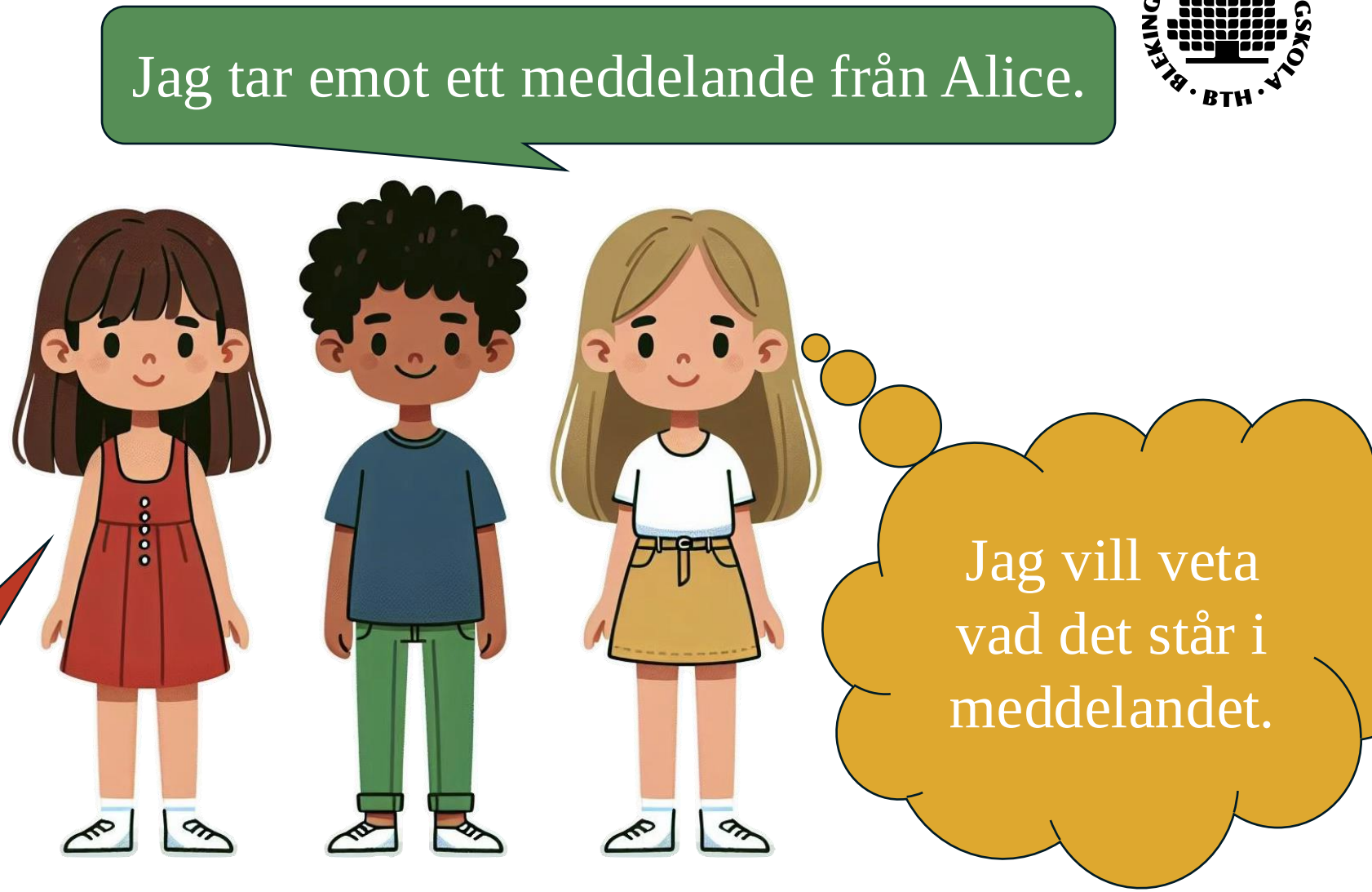
Dagens tema - kryptering

Alice, Bob och Eve kommer att visa oss hur man skapar hemliga meddelanden – så kallade kryptogram. De kommer också att berätta för oss hur man kan göra för att kunna läsa ett krypterat meddelande om man känner till dess nyckel och hur man kan försöka ta reda på vad det står även om man inte känner till nyckeln.

Att kryptera

Att skicka något så att bara den man själv väljer kan läsa vad det står.

Varför vill vi skicka hemliga meddelanden?



Att kryptera

Alice vill skicka ett meddelande till sin vän Bob.

Alice vill se till att det bara är Bob som kan läsa det.

Hon **krypterar** meddelandet och berättar för Bob hur han ska göra för att läsa meddelandet. Hon ger honom **nyckeln**.

Alice förbereder sitt meddelande

När Alice ska kryptera plockar hon bort allt utom bokstäverna. Hon låter alla bokstäver vara små bokstäver.

”Jag bakar bullar.”

Skrivs då:

`jagbakarbullar`

Alice berättar Förskjutningskrypto

Förskjutningskrypto kallas också för Caesar-krypto eftersom den romerska kejsaren Caesar ofta använde krypterade meddelanden.

Man krypterar genom att förskjuta i alfabetet.

Alice skickar ett meddelande Förskjutningskrypto

Om vi har ett **k** och vill kryptera det genom att förskjuta tre steg så kommer vi att få **N** när vi krypterat.

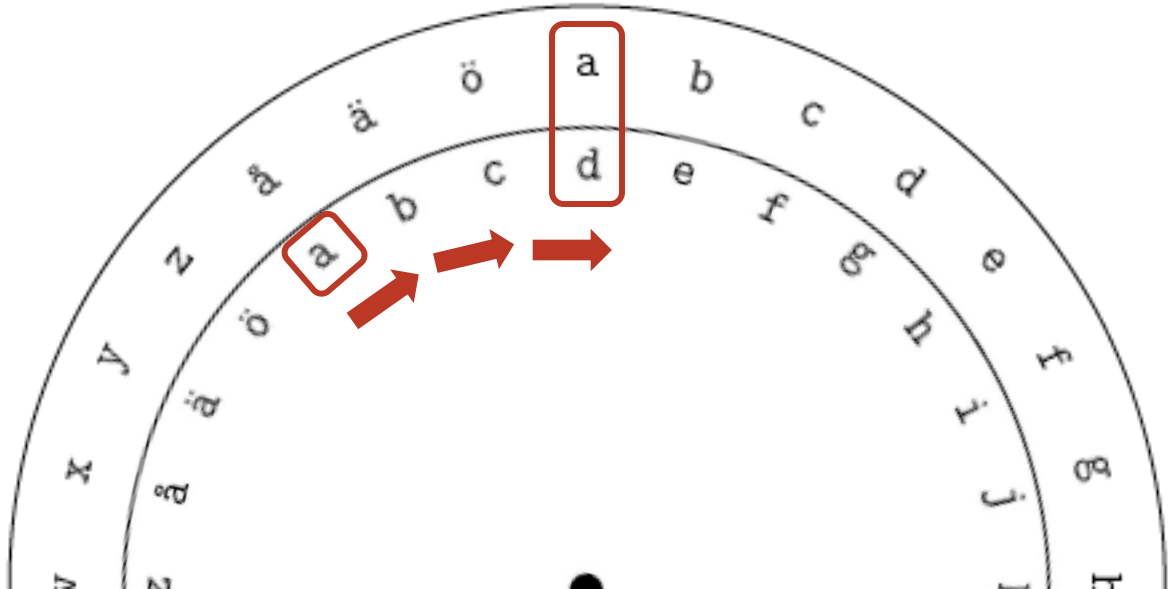
abcdefghijklmnopqrstuvxyzåäö

Om **w** finns i en text så ersätter vi det med **v**.

Alice skickar ett meddelande
Förskjutningskrypto

abcdefghijklmnopqrstuvxyzåäö

Vi förskjuter varje bokstav.
Här är förskjutningen tre steg.



Alice skickar ett meddelande Förskjutningskrypto

Om vi inte vill använda kryptosnurran så kan vi räkna på förskjutningen. Då måste vi omvandla varje bokstav till ett tal.

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alice skickar ett meddelande
Förskjutningskrypto

Alice vill skicka meddelandet:

Jag bakar bullar. **`jagbakarbullar`**

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alice skickar ett meddelande
Förskjutningskrypto

j	a	g	b	a	k	a	r	b	u	l	l	a	r
9	0	6	1	0	10	0	17	1	20	11	11	0	17

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alice skickar ett meddelande
Förskjutningskrypto

j	a	g	b	a	k	a	r	b	u	l	l	a	r
9	0	6	1	0	10	0	17	1	20	11	11	0	17
+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
12	3	9	4	3	13	3	20	4	23	14	14	3	20

Jag adderar 3 till varje tal. Då får jag nya tal som jag ska översätta till bokstäver igen.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alice skickar ett meddelande
Förskjutningskrypto

j	a	g	b	a	k	a	r	b	u	l	l	a	r
9	0	6	1	0	10	0	17	1	20	11	11	0	17
+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
12	3	9	4	3	13	3	20	4	23	14	14	3	20
M	D	J	E	D	N	D	U	E	Y	O	O	D	U

Kryptogram:
MDJEDNDUEYOODU
Nyckel: 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

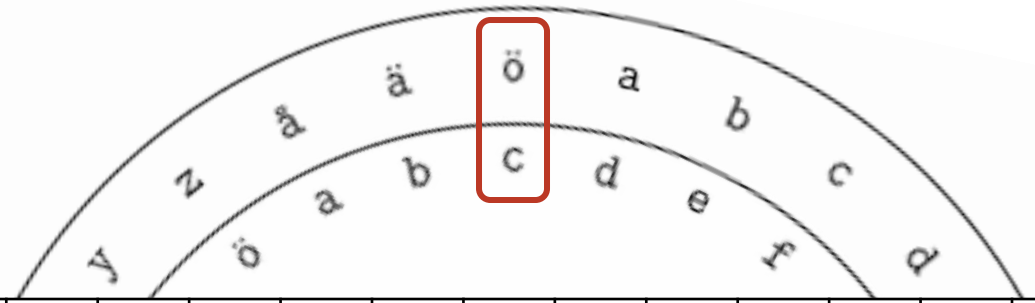
Alice vill berätta något!
Förskjutningskrypto

Om Alice vill skriva **bröd** istället för bullar så dyker det upp ett problem.

Om jag använder snurran när jag krypterar **Ö** så får jag ett **c** i kryptogrammet.

	k	a	r	b	r	ö	d
	10	0	17	1	17	27	3
	+3	+3	+3	+3	+3	+3	+3
	13	3	20	4	20	30	6
	N	D	U	E	U	?	G

30-28=2



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Alice skickar ett meddelande
Förskjutningskrypto

j	a	g	b	a	k	a	r	b	u	l	l	a	r
9	0	6	1	0	10	0	17	1	20	11	11	0	17
+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
12	3	9	4	3	13	3	20	4	23	14	14	3	20
M	D	J	E	D	N	D	U	E	Y	O	O	D	U

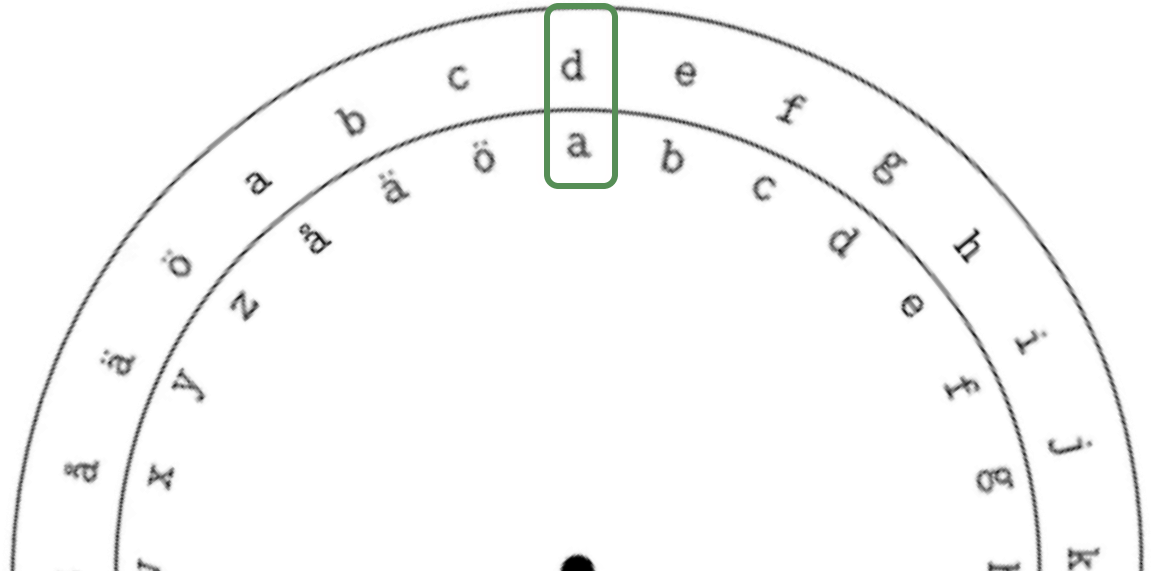
Kryptogram: MDJEDNDUEYOODU
Nyckel: 3

Alice skickar sitt kryptogram till Bob.

Bob dekrypterar meddelandet
Förskjutningskrypto

abcdefghijklmnopqrstuvxyzåäö

Nu förskjuts bokstäverna åt andra hållet.



Bob dekrypterar meddelandet Förskjutningskrypto

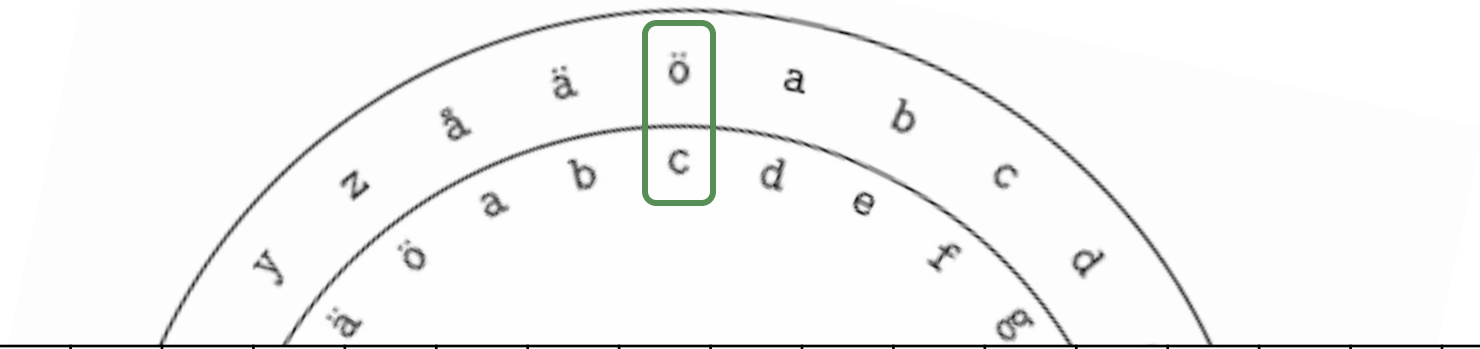
M	D	J	E	D	N	D	U	E	Y	O	O	D	U
12	3	9	4	3	13	3	20	4	23	14	14	3	20
-3	-3	-3	-3	-3	-3	-3	-3	-3	-3	-3	-3	-3	-3
9	0	6	1	0	10	0	17	1	20	11	11	0	17
j	a	g	b	a	k	a	r	b	u	l	l	a	r

Klartext: jagbakarbullar

Nu vet Bob att Alice bakar bullar till deras fredagsfika!

Bob vill berätta något!
Förskjutningskrypto

Om Bob ska dektyptera kryptogrammet som innehåller ordet **bröd** så måste han justera det tal han får för att kunna översätta till en bokstav.
När **c** ska dekrypteras får vi 2-3=-1. Här får vi addera 28. Då får vi 27 som är **ö**.



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	å	ä	ö
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Eve vill knäcka kryptogrammet Förskjutningskrypto

Klartext:
jagbakarbullar

Kryptogram:
MDJEDNDUEYOODU

Jag **krypterar** mitt meddelande och skickar kryptogrammet till Bob.

Kryptogram:
MDJEDNDUEYOODU

Hur ska jag få veta vad det står?

Kryptogram:
MDJEDNDUEYOODU

Klartext:
jagbakarbullar

Jag **dekrypterar** så att jag kan läsa meddelandet jag fick av Alice.

Eve vill knäcka kryptogrammet Förskjutningskrypto

M	D	J	E	D	N	D	U	E	Y	O	O	D	U
12	3	9	4	3	13	3	20	4	23	14	14	3	20

Eve måste försöka med många olika nycklar.
Hur många finns det?


BLEKINGE TEKNISKA HÖGSKOLA
BTH