

UiO : Department of Informatics
University of Oslo

IN1020 – Gruppe 14



Kryptering

- Algoritme
- Nøkkel



Eks.: Cæsarschiffer

- Algoritme:
  - Skifte bokstavene fremover eller bakover i alfabetet et gitt antall plasser
- Nøkkel:
  - Hvor mange plasser det skal flyttes

Eks.: Cæsarschiffer

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Schiffertekst = RE ZJCNELAN RAÅ ÅZCCNU

- Nøkkel = 4
- Klartekst = VI ANGRIPER VED DAGGRY

Skytale

- Fra antikkens Sparta (omkring 500 f.kr.)

- Algoritime: «skriv meldingen på en lærreim surret rundt en stokk»
  - (Betyr egentlig det samme som «hver x-te bokstav står på samme linje»)
- Nøkkel: tykkelsen på stokken

Kryptering

- Algoritme
- Nøkkel
- Symmetrisk/asymmetrisk



Symmetrisk

- Samme nøkkel er brukt både for kryptering og dekryptering
- Forutsetter at både sender og mottaker kjenner til nøkkelen på forhånd
- Mer tidseffektiv enn asymmetrisk

Asymmetrisk

- «En» offentlig og en privat nøkkel
- En melding som er kryptert med offentlig nøkkel kan kun dekrypteres med privat nøkkel
- Trenger ikke å kjenne til nøkkel på forhånd
- Mindre tidseffektiv enn symmetrisk

Asymmetrisk kryptering - kryptere



Omid ønsker å sende en melding til Kristin



Klartekst

Eksamen i IN1020
Høsten 2020

Chiffertekst

27fdbe64 8588b3d1
21ed8e8e ed01c340
982c50a4 8d87c7b2

Kryptere meldingen med Kristin sin offentlige nøkkel

Kristin sin offentlige nøkkel



Asymmetrisk kryptering - dekryptere



Kristin mottar chiffertekst fra Omid



Chiffertekst

27fdbe64 8588b3d1
21ed8e8e ed01c340
982c50a4 8d87c7b2

Kristin sin private nøkkel

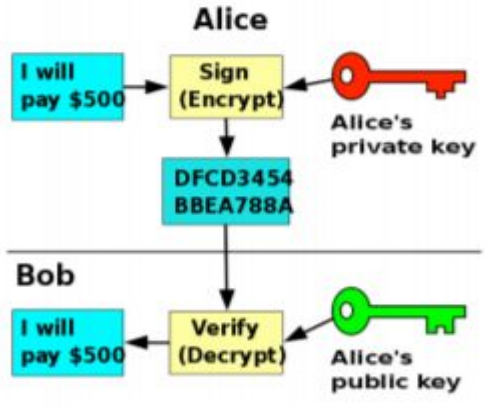


Klartekst

Eksamen i IN1020
Høsten 2020

Digital signatur

- Genereres med privat nøkkel
- Verifiseres med offentlig nøkkel
- Bekrefter mottakers identitet og at meldingen ikke er tuklet med



EKSAMENSOPPGAVER

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

A. Erna skal sende Siv et konfidensielt dokument, som det er viktig at beskyttes mot innsyn fra andre. Hvilken nøkkel må Erna benytte for å kryptere dokumentet før det sendes til Siv?
Velg ett alternativ:

- Ernas private nøkkel
- Ernas offentlige nøkkel
- Sivs offentlige nøkkel
- Sivs private nøkkel

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

A. Erna skal sende Siv et konfidensielt dokument, som det er viktig at beskyttes mot innsyn fra andre. Hvilken nøkkel må Erna benytte for å kryptere dokumentet før det sendes til Siv?
Velg ett alternativ:

- Ernas private nøkkel
- Ernas offentlige nøkkel
- Sivs offentlige nøkkel ✔
- Sivs private nøkkel

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

B. Siv har utarbeidet et dokument som skal godkjennes og signeres digitalt av Erna før det er gyldig. Erna har fått tilsendt det digitale dokumentet, og vil signere det ved hjelp av asymmetrisk kryptering. Hvilken nøkkel skal Erna benytte når hun foretar det som kalles *digital signering*?

Velg ett alternativ

- Ernas private nøkkel
- Ernas offentlige nøkkel
- Sivs private nøkkel
- Sivs offentlige nøkkel

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

B. Siv har utarbeidet et dokument som skal godkjennes og signeres digitalt av Erna før det er gyldig. Erna har fått tilsendt det digitale dokumentet, og vil signere det ved hjelp av asymmetrisk kryptering. Hvilken nøkkel skal Erna benytte når hun foretar det som kalles *digital signering*?

Velg ett alternativ

- Ernas private nøkkel ✔
- Ernas offentlige nøkkel
- Sivs private nøkkel
- Sivs offentlige nøkkel

Jobbe med ukesoppgaver og stille spørsmål :)

Ukens filmtips

Me, Earl and the Dying girl



Hastighet eksempel

Filen som skal lastes opp er 800 MB.

Hastigheten på opplastning er 50 Megabit per sekund.

1 megabit per sekund er det samme som 0,125 Megabytes per sekund.

50 * 0,125 = 6,25. Det vil si 6,25 Megabytes per sekund i opplastingshastighet.

For å finne ut hvor lang tid det tar å laste opp hele filen deler vi antallet, 800 MB, på antallet megabytes per sekund i opplastingshastighet.