NTNU

Norwegian University of Science and Technology

Intro til Kryptografi

Abel-leir 2020

Tjerand Silde

NTNU Applied Cryptology Lab &
Institutt for Matematiske Fag

09. Januar 2020

NTNU

Oversikt

- Diskrete Logaritmer
- Nøkkelutveksling
- Kryptering
- Hashfunksjoner
- Digitale Signaturer

NTNU

Diskrete Logaritmer I

Formål:
Sikkerheten til kryptografiske protokoller er basert på vanskelige matematiske problemer.

NTNU

Diskrete Logaritmer II

Diskrete logaritmer:

- Velg en gruppe $\mathbb{G}$ av primsk orden q med generator g
- Velg et tilfeldig tall $a \in [1, ..., q-1]$ og la $h = g^a$
- Gitt g og a, da er det enkelt å beregne h
- Gitt g og h, da er det vanskelig å beregne a

NTNU

Nøkkelutveksling I

Formål:
To personer ønsker å bli enige om en felles hemmelig nøkkel ved å kommunisere over en åpen kanal.

NTNU

Nøkkelutveksling II

Diffie-Hellman nøkkelutveksling:

- Velg en gruppe $\mathbb{G}$ av primsk orden q med generator g

- Person A velger et tilfeldig tall $a \in [1, ..., q-1]$ og beregner $h_1 = g^a$
- Person B velger et tilfeldig tall $b \in [1, ..., q-1]$ og beregner $h_2 = g^b$

- A sender h_1 til B og B sender h_2 til A
- A beregner $k_s = h_2^a$ og B beregner $k_s = h_1^b$

- Den hemmelige nøkkelen er $k_s = g^{ab}$

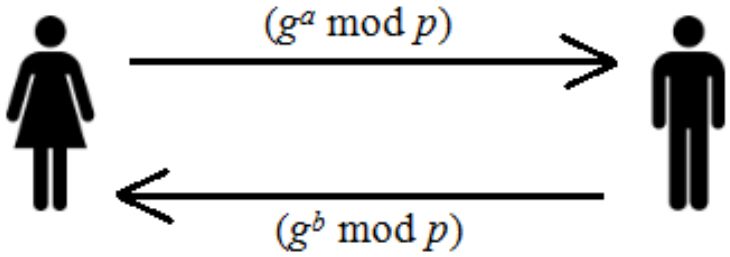
Nøkkelutveksling III

Alice

Known numbers: p, g, a

Bob

Known numbers: p, g, b



NTNU

Kryptering I

Formål:
En person ønsker å sende en hemmelig melding til en annen person over en åpen kanal.

Kryptering II

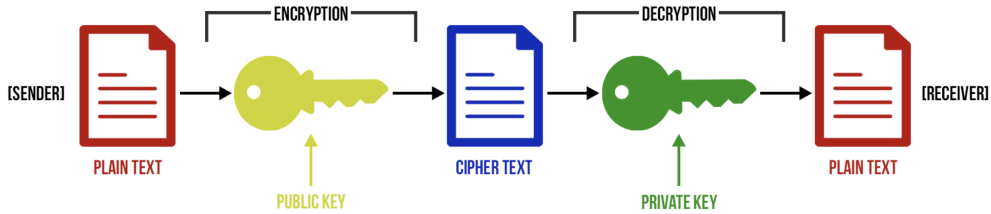
Et offentlig-nøkkel krypteringssystem er en protokoll for to personer med funksjonene $\texttt{Enc}(\cdot,\cdot)$ og $\texttt{Dec}(\cdot,\cdot)$ sammen med en offentlig nøkkel k_p og en hemmelig nøkkel k_s:

— $\texttt{Enc}$ tar som input en offentlig nøkkel k_p og en melding m, og returnerer en chiffertekst c: $\texttt{Enc}(k_p, m) = c$.

— $\texttt{Dec}$ tar som input en hemmelig nøkkel k_s og en chiffertekst c, og returnerer en melding m: $\texttt{Dec}(k_s, c) = m$.

Alle kan kryptere en melding, men bare en person kan dekryptere chifferteksten.

Kryptering III



NTNU

Kryptering IV

El-Gamal kryptosystemet:

- Velg en gruppe $\mathbb{G}$ av primsk orden q med generator g
- Velg et tilfeldig tall $a \in [1, ..., q-1]$ og beregn $h = g^a$
- Den offentlige nøkkelen k_p er gruppeelementet h
- Den hemmelige nøkkelen k_s er tallet a

Kryptering V

El-Gamal kryptosystemet:

— Kryptering av en melding $\texttt{Enc}(h, m)$:
- Velg et tilfeldig tall $b \in [1, ..., q-1]$
- Beregn $c_1 = g^b$ og $c_2 = m \cdot h^b$
- Returner $c = (c_1, c_2)$

— Dekryptering av en chiffertekst $\texttt{Dec}(a, c)$:
- Beregn $c_2 / c_1^a = m$

NTNU

Hashfunksjoner I

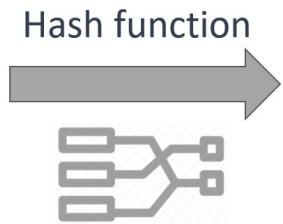
En hashfunksjon `H` er en deterministisk funksjon som tar en vilkårlig verdi og returnerer en verdi av en gitt lengde. En hashfunksjon har de tre følgende egenskapene:

- *Collision resistance*,
- *Pre-image resistance*,
- *Second pre-image resistance*.

Hashfunksjoner II

Text

Some text
Some text
Some text
Some text
Some text
Some text
Some text



Hash value

20c9ad97c081d63397d
7b685a412227a40e23c
8bdc6688c6f37e97cfbc2
2d2b4d1db1510d8f61e
6a8866ad7f0e17c02b14
182d37ea7c3c8b9c2683
aeb6b733a1

NTNU

Hashfunksjoner III

Collision resistance:
Det må være vanskelig å finne to forskjellige verdier m_1 og m_2 slik at $\mathtt{H}(m_1) = \mathtt{H}(m_2)$.

NTNU

Hashfunksjoner IV

Pre-image resistance:
Gitt en hashverdi h så må det være vanskelig å finne en verdi m slik at $h = \mathtt{H}(m)$.

NTNU

Hashfunksjoner V

Second pre-image resistance:
Gitt en verdi m_1 så må det være vanskelig å finne en annen verdi m_2 slik at $\mathtt{H}(m_1) = \mathtt{H}(m_2)$.

NTNU

Digitale Signaturer I

Formål:
En person ønsker å være sikker på at en melding han har mottatt faktisk er sendt fra en annen gitt person.

NTNU

Digitale Signaturer II

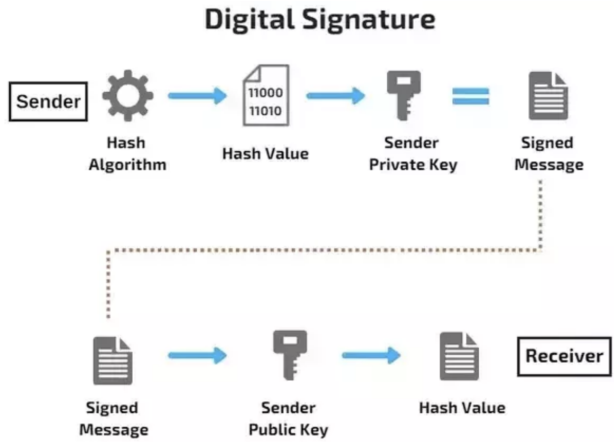
Et digitalt signatursystem er en protokoll for to personer med funksjonene $\texttt{Sign}(\cdot,\cdot)$ og $\texttt{Verify}(\cdot,\cdot,\cdot)$ sammen med en hashfunksjon $\texttt{H}$, en offentlig nøkkel k_p og en hemmelig nøkkel k_s:

— $\texttt{Sign}$ tar som input en hemmelig nøkkel k_s og en melding m, og returnerer en signatur σ: $\texttt{Sign}(k_s, m) = \sigma$.

— $\texttt{Verify}$ tar som input en offentlig nøkkel k_p, en signatur σ og en melding m, og returnerer en verdi **1** eller **0**: $\texttt{Verify}(k_p, \sigma, m) = \mathbf{1} \vee \mathbf{0}$.

Bare én person kan signere en melding, men alle kan verifisere en signatur.

Digitale Signaturer III



NTNU

Digitale Signaturer IV

Schnorr signatursystemet:

- Velg en gruppe $\mathbb{G}$ av primsk orden q med generator g
- Velg en hashfunksjon H som sender verdier til $\mathbb{G}$
- Velg et tilfeldig tall $a \in [1, ..., q-1]$ og beregn $h = g^a$
- Den offentlige nøkkelen k_p er gruppeelementet h
- Den hemmelige nøkkelen k_s er tallet a

Digitale Signaturer V

Schnorr signatursystemet:

— Signering av en melding $\texttt{Sign}(a, m)$:
- Velg et tilfeldig tall $b \in [1, ..., q-1]$
- Beregn $d = g^b$ og $e = \texttt{H}(d|m)$
- Beregn $f = b - ae$
- Returner $\sigma = (e, f)$

— Verifisering av en signatur $\texttt{Verify}(h, \sigma, m)$:
- Beregn $d' = g^f h^e$ og $e' = \texttt{H}(d'|m)$
- Dersom $e \stackrel{?}{=} e'$ returner **1** ellers returner **0**

NTNU

Takk! Spørsmål?

E-post: tjerand.silde@ntnu.no
Slides: `www.tjerandsilde.no/talks`