Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 2: Kryptografi

Spørsmål 1

a. For hvilke informasjonstilstander (lagring, overføring, behandling) kan kryptografi brukes til å beskytte informasjon?
b. Hvilke sikkerhetstjenester kan støttes av kryptografi?

Spørsmål 2

Alice ønsker å sende melding *M* til Bob, uten at Eve observere den. Alice og Bob har blitt enige om å bruke en symmetrisk kryptoalgoritme. Nøkkelutveksling er allerede gjort, slik at de har felles nøkkel *K* for den spesifikke krypteringsalgoritmen E.

a. Beskriv trinnene Alice må følge for å kryptere *M* og sende chifferteksten til Bob.
b. Beskriv trinnene som Bob må følge for å dekryptere den mottatte chiffertekst *C*.

Spørsmål 3

Alice ønsker å sende en melding *M* med en meldingsautentiseringskode MAC(*M*) til Bob. Alice og Bob deler en hemmelig nøkkel *k*, og har blitt enige om å bruke en bestemt algoritme MACfunc som tar inndataparametere *M* og *k* for å produsere MAC(*M*).

a. Beskriv trinnene Alice må følge for å sende *M* .
b. Beskriv trinnene som mottaker Bob må følge for å verifisere autentisiteten til *M*.
c. Forklar hvorfor en MAC beviser for Bob at den mottatt melding er autentisk, og hvorfor Bob **ikke er istand** til å bevise overfor en tredjepart at meldingen er autentisk.

Spørsmål 4

Alice ønsker å sende melding *M* med digital signatur Sig(*M*) til Bob. De har hverandres offentlige nøkler, og har blitt enige om en kryptografisk hash-funksjon h og en signatur-algoritme som opererer i signeringsmodus S (tilsvarende dekrypteringsmodus D) eller i verifiseringsmodus V (tilsvarer krypteringsmodus E).

a. Beskriv trinnene Alice må følge for å sende *M*.
b. Beskriv trinnene som mottaker Bob må følge for å verifisere autentisiteten av *M*.
c. Forklar hvorfor den digitale signaturen beviser for Bob at den mottatte meldingen er autentisk, og hvorfor Bob **er istand** til å bevise overfor en tredjepart at meldingen er autentisk.
d. Hvordan kan en avsender gi en plausibel grunn til å nekte for (avvise) å ha sendt en signert melding?
e. Diskuter den semantiske tolkningen av "digitalt signert melding", som kan bety: I) at jeg Alice er enig i innholdet av meldingen, eller II) Alice sendte meldingen uten nødvendigvis å være enige i innholdet?

Spørsmål 5

Anta at en binær additiv strømchiffer-algoritme (som bruker en pseudotilfeldig nøkkelstreng eller en engangsnøkkel (One-Time-Pad)) har blitt brukt til å kryptere en elektronisk pengetransaksjon. Anta at det ikke brukes andre kryptografiske mekanismer. Forklar hvordan en angriper kan endre overføringsbeløpet uten å vite noe om nøkkelen som brukes (du kan anta at angriperen vet formatet på klartekstmelding som brukes ved overføring av pengene.)

Spørsmål 6

Hash-funksjoner brukes ofte til å verifisere meldingsintegritet.

a. Oppgi fire fundamentale krav til kryptografiske hash-funksjoner.
b. Hva er forskjellen mellom de to variantene av kollisjonsresistens?
c. Bruk Internett til å finne en SHA-2 demo webside. Du finner en interaktiv webside laget av Geraint Luff som kan finnes på: http://geraintluff.GitHub.io/sha256/
   Undersøk hash-funksjons egenskaper ved å beregne SHA-2 hash for følgende:
   (i) ta ut $100 fra min konto
   (II) ta ut $1000 fra min konto
   (III) ta ut $100 fra din konto
   (IV) (du kan prøve å lage hashe for både lengre og kortere meldinger)

Spørsmål 7

Anta at vi krever at melding skal sendes med både konfidensialitet **og** integritet/autentisitet/uavviselighet: I hvilken rekkefølge bør signatur-funksjonen og krypteringsfunksjonen brukes? Også forklare hvorfor den rekkefølgen er fornuftig.

Spørsmål 8

Diffie-Hellman-algoritmen for nøkkelgenerering lar to parter opprette en felles hemmelig nøkkel uten at de på forhånd har det.

a. Forklar med formell notasjon trinnene i Diffie-Key-algoritmen.
b. Forklar hvorfor Diffie-Hellman-algoritmen i seg selv ikke gir gjensidig autentisering av partene, dvs. hvorfor den ikke gir partene gjensidig informasjon om hvem som deltar.

Spørsmål 9

Kvantecomputing har potensiale til å knekke de fleste standardiserte asymmetriske kryptografiske algoritmer. Kvanteresistente kryptoalgoritmer kalles PQC (Post-Quantum Crypto) fordi de skal være sikre selv etter at store kvantecomputere er tilgjengelige på marketed. Anta følgende tidsperioder:

- t_1: tiden det tar å standardisere kvanteresistente kryptoalgoritmer (PQC).
- t_2: tiden det tar å oppdatere krypto-applikasjoner med standardiserte PQC-algoritmer.
- t_3: tiden som eldre ikke-PQC programvare og systemer må forbli operative og sikre
- t_4: tiden det tar å gjøre store kvantecomputere tilgjengelige og praktiske

a. Uttrykke i forhold til ulikhets-ligninger med vilkårene t_1, t_2, t_3 og t_4 to scenarier:
   i. scenario 1 der krypto programmer vil forbli sikre
   ii. Scenario 2 der krypto-applikasjoner blir usikre
b. Hva er forventet tidsramme for standardisering av PQC-algoritmer? Se http://CSRC.NIST.gov/Groups/St/post-Quantum-Crypto/Documents/pqcrypto-2016-Presentation.PDF