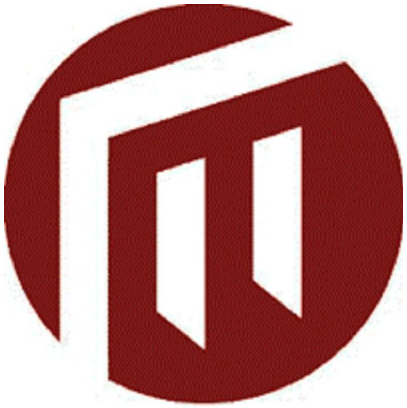


MALMÖ HÖGSKOLA
Centrum för teknikstudier

Trådlösa nätverk, säkerhet och kryptering

Wireless networks, security and cryptography

Examensarbete datavetenskap 15 högskolepoäng
VT 2008

Detta examensarbete i datavetenskap är utfört som en del av högskoleingenjörsutbildningen i programvaruteknik vid Malmö Högskola.

Författare: Andreas Ahlfors

Handledare: Bengt J Nilsson

Resumé

Användandet av trådlösa nätverk breder ut sig mer och mer både bland företag och privatpersoner. För privatpersoner kan det vara skönt att slippa sladdarna som ett vanligt nätverk för med sig och för företag kan det trådlösa nätverket fungera som ett komplement till det vanliga i miljöer där man inte kan eller vill använda vanliga nätverk. Det är ett smidigt sätt att koppla upp sig mot ett nätverk utan att vara fysiskt ansluten till det. Smidigheten har dock ett pris i form av att det är lättare att avlyssna trådlösa nätverk i och med att kommunikationen går genom etern och det saknas fysiskt skydd i form av byggnader och lås som finns för traditionella nätverk. Med tanke på detta är det viktigt att man säkrar nätverket på ett ordentligt sätt.

I detta arbete har jag studerat trådlösa nätverk; hur de fungerar, vilka hot som kan finnas och vad man kan göra för att skydda sig. Detta innefattar standarden 802.11 för trådlösa nätverk samt TCP/IP-modellen för datakommunikation. Kryptering, symmetrisk och asymmetrisk sådan, hur dessa fungerar, vad de används till och skillnaderna dem emellan gås igenom. Olika säkerhetshot mot trådlösa nätverk och säkerhetslösningar i form av WEP, WPA och WPA2 har tagits upp. Avslutningsvis beskrivs kvantkryptering som är en metod för att på ett säkert sätt med hjälp av fysikens lagar överföra en krypteringsnyckel mellan två parter.

Abstract

The use of wireless networks increases among both companies and individuals. For individuals it can be nice to get rid of the cables that fixed networks use and for companies the wireless network can be a complement to the fixed one in environments where you cannot or do not want to use that technique. It is a convenient way to connect to a network without having to be physically connected to it. The convenience however comes at a price as it is easier to tap wireless networks since the communication passes through the ether and there is a lack of physical protection such as buildings and locks that exists for traditional networks. In view of this it is important to secure the network in a proper way.

In this paper, I have studied wireless networks; how they work, which threats that exist and what one can do in order to protect them. This includes the 802.11 standard for wireless networks and the TCP/IP model for data communication. Encryption, both symmetric and asymmetric, how they work, what they are used for and the differences between them is described. Different security threats against wireless networks and security solutions in the forms of WEP, WPA and WPA2 are also reviewed. In conclusion quantum cryptography, which is a method for transmitting a cryptographic key in a secure way by the help of physics, is described.

Innehållsförteckning

1. Inledning

1.1 Trådlösa nätverk – WLAN

Som man hör på namnet så är ett trådlöst nätverk eller WLAN (Wireless Local Area Network) ett nätverk där man inte behöver använda sig av några kablar för att koppla upp sig mot andra datorer, skrivare eller Internet. Istället används radiovågor för att skicka och ta emot data. Trådlösa nätverk är i dagsläget vanligt förekommande både för privatpersoner, företag och på offentliga platser såsom skolor, bibliotek och flygplatser.

Det första trådlösa nätverket, ALOHAnet, togs fram på University of Hawaii 1970 och bestod av sju datorer och kopplade ihop datorer på fyra öar som kommunicerade med en huvuddator på ön Oahu. 1985 började industrin ta fram en ny generation trådlösa lokala nätverk och 1990 startade kommersiell utveckling av WLAN då företaget AT&T släppte WaveLAN. 1991 höll IEEE (se kapitel 1.2) sin första workshop angående trådlösa LAN och deras 802.11-kommitté hade precis påbörjat sitt arbete att ta fram en standard för WLAN. 1996 började tekniken bli mogen och 1997 standardiserades WLAN genom standarden 802.11 som togs fram av IEEE, mer om denna längre fram. I början var hårdvaran så dyr att tekniken endast användes där det var svårt eller omöjligt att använda sig av vanliga nätverk men detta förändrades mot slutet på 90-talet.

För att klienter ska kunna koppla upp sig mot ett trådlöst nätverk krävs det att deras datorer är utrustade med ett trådlöst nätverkskort. En basstation eller accesspunkt kopplar ihop det trådlösa nätverket med det vanliga trådade. Denna accesspunkt fungerar som en knutpunkt i det trådlösa nätverket och samordnar kommunikationen mellan enheterna och mot externa nät som Internet. Beroende på hur stort område det trådlösa nätverket ska täcka så är det möjligt att det inte räcker med en accesspunkt. För att man ska kunna flytta sig runt fritt används en teknik som kallas reassociation. Denna innebär kortfattat att flera olika accesspunkter uppfattas som ett enda nät och om signalen blir för svag från någon av dessa kan den trådlösa enheten byta accesspunkt om den då får en bättre signal från en annan. Detta är inget som användaren själv behöver tänka på utan det sköts automatiskt.

Man pratar om två olika typer av lokala nätverk, infrastrukturnätverk och ad hoc-nätverk. Infrastrukturnätverk är det som beskrivits ovan där man via ett trådlöst nätverk kopplar upp sig mot ett vanligt trådat nätverk. I ett ad hoc-nätverk har man ingen accesspunkt utan två eller flera enheter, till exempel bärbara datorer, kopplar upp sig direkt mot varandra. Detta kallas också peer-to-peer eller IBSS (Independent Basic Service Set). Detta nätverk existerar enbart så länge enheterna är sammankopplade. När det gäller infrastrukturlösningar så finns det två olika varianter, BSS och ESS. BSS (Basic Service Set) är grundstrukturen i ett trådlöst nätverk och består av ett antal trådlösa enheter och en accesspunkt som ger tillgång till Ethernet (standard för trådade nätverk) för alla enheter. Ett Extended Service Set (ESS) består av flera BSS som sammankopplas via Ethernet. En trådlös användare kan förflytta sig mellan olika BSS och byta accesspunkt automatiskt (se reassociation ovan). Flera accesspunkter kan också överlappa varandra och genom att sända på olika kanaler öka bandbredden. WLAN är bara en teknik för trådlösa nätverk. Andra tekniker som kan nämnas är bluetooth, GPRS och IR. Det finns också andra standarder som påminner om WLAN. [6, 7, 8, 10]

Wi-Fi, som inte är någon förkortning, är en benämning för trådlösa nätverk som är baserade på standarder inom 802.11-familjen. Framförallt används det som ett mer slagkraftigt namn för WLAN över 802.11-standarden. Syftet är att genomföra tester och därefter certifiera produkter som fungerar tillsammans. Varumärket Wi-Fi ägs av Wi-Fi Alliance som är en sammanslutning av oberoende företag. Tillverkare som är medlemmar i Wi-Fi Alliance och vars produkter klarar testerna får lov att märka sina produkter med Wi-Fi-logon. [9]

Två begrepp som kommer att användas i uppsatsen är SSID (Service Set IDentifier) som är det samma som ett nätverksnamn och MAC-adress (Media Access Control). En MAC-adress är en unik

identifierare för nätverkskort. Alla nätverkskort har en egen adress som består av sex bytes där de tre första anger tillverkaren och de tre sista anger det enskilda kortet. [3]

1.2 IEEE 802.11

IEEE som är en förkortning av Institute of Electrical and Electronics Engineers är en internationell icke vinstdrivande organisation för elektricitetsrelaterad teknik. Organisationen grundades 1963 och har 365 000 medlemmar i cirka 150 länder. IEEE tar fram industristandarder inom olika teknikområden. 802.11 är en samling standarder för datakommunikation via trådlösa nätverk (WLAN) med frekvenser i 2,4 och 5 GHz-området. Listan över standarderna nedan är inte komplett utan ett urval av de vanligaste. Räckvidderna som nämns nedan gäller vid användning inomhus och påverkas av antal väggar som måste passeras och även materialet i dessa. Hastigheterna som nämns är teoretiska maxhastigheter och de faktiska hastigheterna kan skilja sig väsentligt från dessa. [11, 12, 13]

802.11-1997
Är originalversionen av standarden och kom 1997. Här specificerades två hastigheter; 1 respektive 2 megabits per sekund (Mbit/s) vid frekvensen 2,4 Gigahertz (GHz) eller via IR (infrarött ljus). Räckvidden ligger på cirka 20 meter.

802.11a
Kom 1999 och bygger på originalstandarden. Använder frekvensen 5 GHz samt har en maximal dataöverföringshastighet på 54 Mbit/s. Räckvidden beräknas till cirka 35 meter.

802.11b
Standardiserades även denna under 1999 och bygger precis som 802.11a på originalstandarden. Maximala överföringshastigheten ligger på 11 Mbit/s och använder frekvensen 2,4 GHz. Den har en ungefärlig räckvidd på runt 40 meter. Enheter som använder denna standard kan störas av andra produkter som använder denna frekvens såsom mikrougnar, trådlösa telefoner och bluetooth-enheter.

802.11g
Är en vidareutveckling av 802.11b och kom i juni 2003. Frekvensen 2,4 GHz används fortfarande men dataöverföringshastigheten är här 54 Mbit/s. Räckvidden här är samma som för 802.11b. Även här kan störningarna som nämns ovan spela in. 802.11g-hårdvara är fullt bakåtkompatibel med 802.11b-hårdvara. Det ska dock sägas att hastigheten i nätverket sjunker om en användare med 802.11b-standarden ansluter.

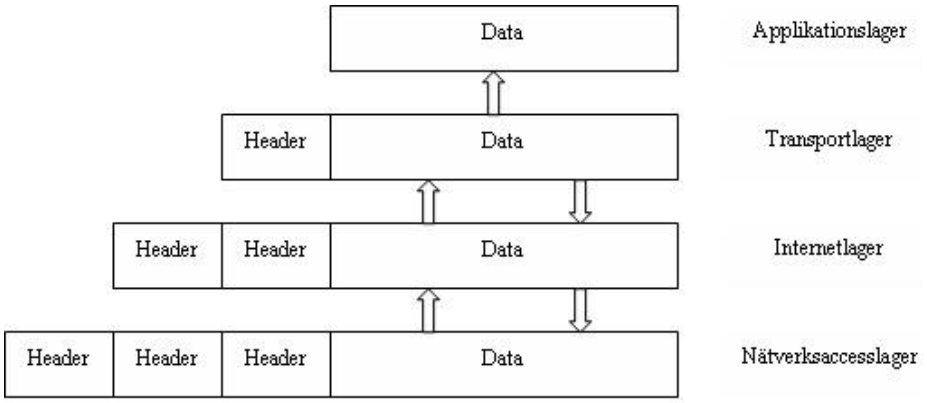
802.11i
Denna standard behandlar säkerhet och är en efterföljare till den tidigare säkerhetsstandarden WEP (se 4.1) som visat sig ha stora brister. WPA (se 4.2), som introducerats av WiFi Alliance, är en annan säkerhetsstandard som implementerar delar av 802.11i och sågs som en tillfällig lösning av svagheterna i WEP. WPAs efterföljare, WPA2 (se 4.3), implementerar 802.11i fullt ut. Antogs sommaren 2004.

802.11n
Detta är en ny standard som är under utveckling och förväntas släppas i juni 2009. Överföringshastigheten väntas ligga på upp emot 600 Mbit/s.

1.3 TCP/IP-modellen

TCP/IP (Transmission Control Protocol/Internet Protocol) är en uppsättning protokoll för datakommunikation. De nämnda protokollen är bara två av flera som ingår men eftersom de är två av de viktigare har de fått ge namn åt modellen. TCP/IP-modellen togs ursprungligen fram av USA:s försvarsdepartement på 1970-talet och ledde fram till ARPANET som är en föregångare till dagens Internet. TCP/IP kommunicerar med hjälp av paket. Ett paket är ett block med data som även innehåller den information som behövs för att det ska kunna levereras till rätt mottagare. TCP kontrollerar leveransen av paketen som skickas. I detta ingår att kontrollera så att paketen skickas i rätt ordning, att de kommer fram till mottagaren och att innehållet inte förändrats under vägen. Skulle ett paket inte nå mottagaren eller om ett paket skadats på vägen skickas detta om tills det nått mottagaren i korrekt form. Detta kontrolleras genom att en bekräftelse skickas tillbaka när ett paket mottagits korrekt. IP:s uppgift är att skicka paket från nod till nod i nätverket tills det når rätt mottagare. Paketformatet som används av IP kallas *datagram*. Adresseringen av paketen sköts med hjälp av IP-adresser som är en unik adress på varje dator som är ansluten till Internet. En IP-adress kan till exempel se ut så här, 100.24.48.6. [3, 14]

TCP/IP-modellen består av fyra lager där varje lager består av flera protokoll och sköter vissa delar av kommunikationen. Data från ett ovanliggande lager kapslas in i underliggande lager. Detta innebär att data läggs till för varje steg nedåt i hierarkin. Detta kan liknas vid de ryska dockor där varje docka har en mindre docka inuti. Dockorna motsvaras här av headers. En header innehåller information som behövs för att paketet ska kunna skickas på ett korrekt sätt till rätt mottagare. Detta kan till exempel vara adressen till mottagaren eller en checksumma. Så för varje lager i TCP/IP-hierarkin som ett paket passerar läggs en ny header till. När sedan paketet tas emot hos mottagaren plockas headern bort i motsvarande lager. På detta sätt kommunicerar varje lager hos den sändande datorn med motsvarande lager hos den mottagande datorn. [15, 16]



Figur 1 Inkapsling [3]

De olika lagren är; applikationslagret (lagret närmast användaren), transportlagret, internetlagret och nätverksaccesslagret. Beroende på i vilket lager data hanteras så har datapaketen olika namn. I applikationslagret kallas det ett meddelande, i transportlagret segment (TCP) eller datagram (UDP), datagram i Internetlagret och slutligen ram i nätverksaccesslagret. Lagren utför följande uppgifter:

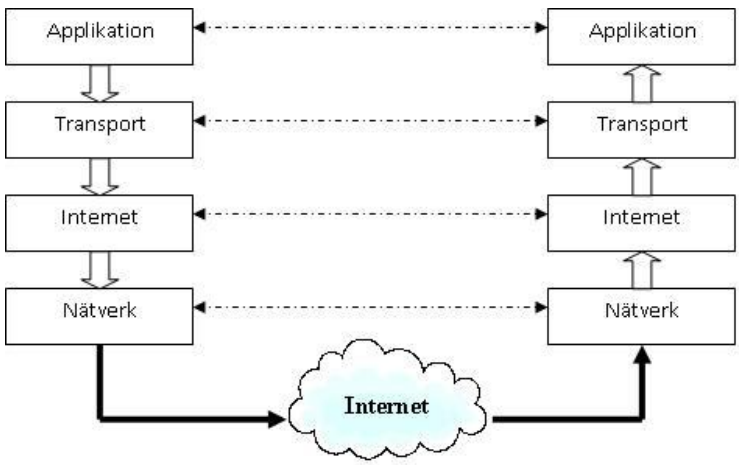
Applikationslagret

Detta lager förser användarapplikationer med de tjänster som behövs för att kommunicera över nätverk. I TCP/IP är en applikation en process som befinner sig ovanför transportlagret. De kommunicerar med hjälp av portar och sockets (se under transportlagret). Andra funktioner som sköts av detta lager är exempelvis kryptering/dekryptering och datakomprimering. Data från applikationen skickas sedan vidare till transportlagret. Protokoll som används på denna nivå är bland annat HTTP som används för att visa webbsidor och FTP som används för filöverföring. [14, 15]

Transportlagret
Transportlagret ansvarar för dataöverföring mellan avsändare och mottagare, det vill säga ser till att paketen kommer till rätt destination. Transportlagret kopplar ihop applikationer genom att använda sig av portar och sockets. En port är en intern adress, ett nummer, som styr vilken applikation som ska ta hand om datan som tas emot. En socket används för att kombinera en IP-adress med ett portnummer. För IP-adressen ovan med data som ska till port 80 så hade dess socket blivit 100.24.48.6:80. De viktigaste protokollen i detta lager är TCP och UDP (User Datagram Protocol). TCP, som beskrivits kort ovan, är ett förbindelseorienterat protokoll för tillförlitlig överföring. Att det är förbindelseorienterat innebär att det kontrollerar att den mottagande datorn är redo att ta emot data innan denna sänds. Tillförlitligheten bygger på de egenskaper som nämndes i inledningen. UDP å andra sidan är ett förbindelselöst protokoll och saknar TCPs förmåga att verifiera att datan nått fram till mottagaren korrekt. Protokollet har dock vissa funktioner för feldetektering som en enkel checksumma. UDP används framför allt till applikationer där överföringshastighet är viktigt och ett tappat paket inte spelar någon större roll. Exempel på detta är strömmad media såsom video och ljud. Båda protokollen skickar data vidare till internetlagret. [14, 15, 16]

Internetlagret
Detta lager ser till att data kan skickas från källa till mål genom ett eller flera nätverk. Det viktigaste protokollet på denna nivå är IP som beskrevs översiktligt i inledningen till detta kapitel. IP används av protokollen i lagren ovanför och under för att skicka data. Det är ett förbindelselöst protokoll och förlitar sig på andra protokoll om tillförlitlig överföring krävs. Adressering av datagram görs med hjälp av IP-adresser. Befinner sig datorerna på samma nätverk skickas datagrammet direkt till rätt dator annars styrs det vidare via routers som kontrollerar IP-adressen och vidarebefordrar det till andra routers tills rätt mottagare nåtts. IP-headern som läggs till i detta lager innehåller bland annat följande information utöver själva datan; avsändarens och mottagarens IP-adress, längden på datan och ett id som används om datan på grund av storlek behöver delas upp i flera paket. Ett annat protokoll i detta lager är ICMP (Internet Control Message Protocol) som är ett felsökningsprotokoll som används för att identifiera problem med sändande av paket. Det använder sig av datagram för att skicka sina meddelanden. [14, 15, 16]

Nätverksaccesslagret
Nätverksaccesslagret är det lägsta lagret och det lager som faktiskt ser till så att datan som ska skickas kommer iväg. Här omvandlas IP-adresser till de fysiska adresser som används av nätverket, MAC-adresser. Datagrammet från Internetlagret tas emot här och utifrån det skapas en ram som är den dataenhet som skickas över nätverket. Ramen innehåller information om avsändare och mottagare (MAC-adresser), längd på datan, själva datan och en checksumma. Ramen omvandlas till bitar och skickas sedan som elektriska signaler eller radiovågor (för trådlösa nätverk). [15, 16]



Figur 2 TCP/IP-modellen [14] (bilden något ändrad)

2. Kryptering

Kryptering, att förvanska information, har ända sedan romartiden varit ett sätt att förhindra obehöriga att ta del av hemlig information. Idag är det fortfarande lika viktigt att kunna skydda information från obehörig åtkomst. I takt med att allt mer information behandlas med hjälp av datorsystem och via Internet ökar också kraven att kunna hålla denna information säker från avlyssning och otillbörlig förvanskning. För att åstadkomma detta är kryptering en viktig beståndsdel. I det följande avsnittet kommer jag att gå igenom hur kryptering fungerar rent allmänt samt förklara en del begrepp.

2.1 Algoritmer och nycklar

Algoritmen är den ena beståndsdelen som behövs för att kunna kryptera ett meddelande. Den anger de regler som gäller vid krypteringen, alltså hur texten ska förvanskas. Detta görs genom att utföra en rad substitutioner och transformationer där man byter ut och ändrar ordningen på de tecken som ingår i meddelandet. Man har en krypteringsalgoritm som sköter krypteringen av meddelandet och en dekrypteringsalgoritm som återställer det ursprungliga meddelandet.

När man pratar om nycklar i samband med kryptering i datorsammanhang så är detta en sekvens av bitar, alltså ettor och nollor. Storleken på nyckeln, hur lång den är, anges oftast i bitar och brukar för symmetrisk kryptering vara mellan 128 och 256 bitar lång. Vid asymmetrisk kryptering är nycklarna längre vilket kommer att förklaras nedan. Ju längre nyckeln är desto svårare är det att knäcka kryptot men det medför också att kryptering och dekryptering tar längre tid. Nycklar kan skapas antingen slumpmässigt med hjälp av en slumptalsgenerator eller med ett lösenord och en algoritm som skapar nyckeln utifrån ditt lösenord. Nyckeln tillsammans med algoritmen styr den kryptotext som genereras. Om samma algoritm används med två olika nycklar kommer kryptotexterna att skilja sig åt. En algoritm utan nyckel kommer inte att ha någon effekt. Det är endast nyckeln som behövs hållas hemlig. Vilken algoritm som använts är alltså inget som behöver hemlighållas. Anledningen till det är att det anses vara orealistiskt att dekryptera ett meddelande utifrån kunskapen om vilken algoritm som använts samt det krypterade meddelandet. [2, 17, 18, 19]

Pfleeger [1] gör en jämförelse mellan algoritmer och nycklar samt lås till hus och nycklar till dessa. Algoritmen kan jämföras med låset. Detta är ett massproducerat standardlås och din granne kan ha ett likadant. (Man tar ju inte fram ett helt unikt lås för varje hus.) Det som däremot är unikt är nyckeln som är olika för varje lås. På samma sätt är algoritmer allmänt kända och samma algoritmer används av många olika personer och företag medan varje kommunikationspar har sin egen privata nyckel för kryptering och dekryptering.

2.2 XOR

XOR (exclusive or) är en binär operation som utförs på bitsträngar. En XOR-operation på två bitsträngar resulterar i en tredje. Om två bitar som jämförs har samma värde blir resultatet 0 och om de har olika värde blir resultatet 1. Detta är en operation som används inom kryptering vilket jag kommer att återkomma till när jag tittar på WEP, WPA och WPA2. Som exempel, för att se hur det fungerar, antag att A är meddelandet som ska krypteras, B är nyckeln och C är kryptotexten. Då fungerar det så här: [3]

A XOR B = C (Klartexten tillsammans med nyckeln ger kryptotexten)
C XOR B = A (Kryptotexten tillsammans med nyckeln ger klartexten)

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Tabell 1 XOR [3]

2.3 Symmetrisk kryptering

Symmetrisk kryptering är även känd under flera andra namn som till exempel secret-key eller single-key kryptering. Metoden kallas så eftersom man använder samma nyckel både för att kryptera och dekryptera meddelanden. Enkelt förklarat fungerar symmetrisk kryptering på följande vis:

1. Avsändaren av meddelandet tar fram sitt meddelande i klartext.

2. Han använder sedan den krypteringsalgoritm som överenskommits med mottagaren tillsammans med den gemensamma nyckeln som de båda har tillgång till för att kryptera meddelandet.

3. Meddelandet kan nu skickas, i krypterad form, till mottagaren.

4. Mottagaren tar emot meddelandet och dekrypterar det med hjälp av en dekrypteringsalgoritm, som fungerar som krypteringsalgoritmen fast omvänt, tillsammans med sin nyckel.

5. Mottagaren kan nu läsa meddelandet i klartext.

Stallings [2] talar om två krav som måste uppfyllas för att symmetrisk kryptering ska kunna användas på ett säkert sätt: algoritmen som används måste vara tillräckligt stark och nycklarna som sändare och mottagare använder måste ha erhållits på ett säkert sätt. Med tillräckligt stark menas att någon obehörig som har fått tillgång till några krypterade meddelanden och som känner till vilken algoritm som använts inte ska kunna dekryptera meddelandena eller lista ut nyckeln. Likaså gäller att om en inkräktare kommit över nyckeln och vet vilken algoritm som använts kan denne läsa meddelandena i klartext.

Block- och strömkrypton

Block- och strömkrypton används båda vid symmetrisk kryptering och kan sägas vara olika metoder att kryptera klartext till kryptotext. Båda uppnår samma resultat, det vill säga att de producerar en krypterad text utifrån en klartext, men sättet de gör det på skiljer sig åt. Båda metoderna använder en nyckel för att kryptera meddelanden. De olika krypteringsalgoritmerna använder sig av någon av metoderna.

Strömkrypton krypterar klartext ett tecken i taget till kryptotext. Vilket resultatet av krypteringen blir beror på tecknet som ska krypteras, nyckeln som används och den algoritm som används. Dessutom är ordningen viktig. Ändrar man ordningen på någon av tecknen i klartexten så kommer den krypterade texten också att bli annorlunda. Några olika strömkrypton är RC4, SEAL och Panama. För vidare information om dessa se Wikipedia [42].
Blockkrypton krypterar till skillnad från strömkrypton inte varje tecken för sig utan ett block i taget. Ett block är ett visst antal bytes och bestäms av algoritmen. Varje block hanteras för sig och det finns inget samband mellan krypteringen av de olika blocken. Ett problem med blockkrypton är att en klartext alltid översätts till samma kryptotext om samma nyckel används. Detta problem avhjälps genom att blockkrypton använder olika krypteringsmetoder, till exempel ECB (electronic codebook) och CBC (cipher-block chaining), vilka styr hur klartexten omvandlas till kryptotext (se Wikipedia [41]). Exempel på blockkrypton är AES (Advanced Encryption Standard) och Blowfish. Hur dessa fungerar förklaras på Wikipedia [43, 44]. [3]

Det finns för- och nackdelar med både ström- och blockkrypton. Fördelarna med strömkrypton är att de är snabba. Detta eftersom varje symbol kan krypteras direkt och inte behöver invänta mer klartext som är fallet med blockkrypton. En annan fördel är att om det blir något fel i krypteringsprocessen så är det bara det aktuella tecknet som påverkas. Nackdelarna är låg diffusion[1] det vill säga att eftersom

[1] Diffusion innebär att information i klartexten sprids ut över hela kryptotexten. Bra diffusion medför att en inkräktare behöver ha tillgång till mer kryptotext för att komma fram till algoritmen.

varje tecken krypteras för sig så finns information om det tecknet bara i ett tecken i kryptotexten. Detta medför också ett annat problem nämligen att någon som knäckt koden kan sätta ihop egna meddelanden och skicka ett nytt meddelande som ser äkta ut. [1]

För- och nackdelarna med blockkrypton är de omvända jämfört med strömkrypton. Fördelarna är alltså att blockkrypton har hög diffusion vilket innebär att eftersom klartexten krypteras i block så är inte varje enskilt tecken lika känsligt som för strömkrypton. Man kan inte heller sätta in enskilda tecken i ett block eftersom längden då skulle bli felaktig och detta skulle upptäckas direkt. Nackdelarna är att blockkrypton är långsammare än strömkrypton eftersom man måste invänta att ett block av tecken blir klart innan kryptering kan ske. Dessutom så kommer ett felaktigt krypterat tecken att påverka hela det blocket. [1]

Ett av problemen med symmetrisk kryptering är hur man ska skicka nycklarna första gången man ska kommunicera eftersom man då inte har någon nyckel att använda. En lösning på detta är att använda asymmetrisk kryptering som beskrivs härnäst.

2.4 Asymmetrisk kryptering

Asymmetrisk kryptering skiljer sig från symmetrisk dito på så sätt att här används två olika nycklar. Man har en privat som endast man själv känner till och en publik nyckel som kan delas ut fritt till de man behöver kommunicera med. Den publika nyckeln behöver alltså inte hållas hemlig. Den används av alla som vill kommunicera med dig. Mottagaren dekrypterar sedan meddelandena med sin privata nyckel. Detta medför den fördelen att man inte behöver ha en nyckel för varje person man kommunicerar med som är fallet vid symmetrisk kryptering. De båda nycklarna fungerar som varandras inverser det vill säga att den ena nyckeln upphäver vad den andra gör. Asymmetrisk kryptering kan liknas vid en brevlåda med lås. Vem som helst kan posta ett brev i brevlådan om man känner till adressen (jämför den publika nyckeln) men endast den som har nyckeln kan öppna den och läsa meddelandena (den privata nyckeln). En skillnad jämfört med symmetriska algoritmer är att asymmetriska är baserade på matematiska funktioner istället för att förändra bit-mönster. Detta tillsammans med att nycklarna är betydligt större vid asymmetrisk kryptering gör att det tar längre tid att använda denna metod. En viktig egenskap med asymmetrisk kryptering är att det ska vara lika svårt att lista ut den ena nyckeln med hjälp av den andra som det är att dekryptera meddelandet utan nyckel. [2, 3, 20, 21]

Nyckelutbyte

Ett av de främsta användningsområdena för asymmetrisk kryptering är för att kryptera nycklar som används för symmetrisk kryptering. Som nämndes tidigare så är ett stort problem med symmetrisk kryptering hur man ska kunna utbyta nycklar på ett säkert sätt. Svaret på detta är alltså asymmetrisk kryptering. Eftersom nyckelstorleken vid symmetrisk kryptering är så mycket mindre än den är vid asymmetrisk så kan den symmetriska nyckeln skickas i ett enda meddelande vilket är bra ur säkerhetssynpunkt. Det fungerar på följande sätt: [1, 3]

1. Mottagaren av meddelandet har tidigare tagit fram två nycklar, en publik och en privat, och publicerat sin publika nyckel så att avsändaren har tillgång till denna.

2. Avsändaren skapar en symmetrisk nyckel som de kommer att använda för kommunikationen i fortsättningen.

3. Avsändaren använder sedan mottagarens publika nyckel för att kryptera den symmetriska. Den symmetriska nyckeln är nu skyddad under översändandet.

4. Avsändaren skickar den symmetriska nyckeln till mottagaren.

5. Mottagaren kan nu dekryptera den översända symmetriska nyckeln med hjälp av sin egen privata nyckel.

6. Den fortsatta kommunikationen mellan parterna krypteras med hjälp av den symmetriska nyckeln.

Jämförelse mellan symmetrisk och asymmetrisk kryptering
Storleken på nycklarna som används vid asymmetrisk kryptering är betydligt större än de nycklar som används vid symmetrisk kryptering. Nyckelstorleken vid symmetrisk kryptering ligger vanligtvis mellan 128 och 256 bitar att jämföras med nycklarna vid asymmetrisk kryptering som ligger mellan 512 och 4096 bitar. Anledningen till dessa skillnader i nyckellängd beror på vad som krävs av en inkräktare för att knäcka kryptot. Tittar man på de symmetriska algoritmerna så innebär en nyckelstorlek på 128 bitar att det finns 2^{128} olika nycklar (eftersom varje bit kan vara antingen 1 eller 0). För att hitta rätt nyckel krävs det i genomsnitt att man testar hälften, det vill säga 2^{127} av dessa vilket tar väldigt lång tid. Eftersom asymmetriska algoritmer är uppbyggda på ett annat sätt än de symmetriska behöver man inte prova alla möjliga nycklar utan man letar istället efter primtal som multiplicerade med varandra, primtalsfaktorer, bildar en del av den publika nyckeln. Detta går ganska fort för mindre tal varför nycklarna vid asymmetrisk kryptering måste vara så mycket större. [20]

Som Stallings [2] nämner är det ingen principiell skillnad på de olika krypteringstypernas motståndskraft mot kryptoanalys utan det som avgör denna är nyckelns storlek samt det uträkningsarbete som krävs för att knäcka kryptot.

	Symmetrisk	Asymmetrisk
Antal nycklar	1	2
Skydd av nyckel	Måste hållas hemlig	Den privata måste hållas hemlig medan den publika kan distribueras fritt
Används till	Allmän kryptering	Nyckelutbyte, autentisering
Nyckeldistribution	Måste utväxlas på säkert sätt	Publika nyckeln kan användas för att distribuera andra nycklar
Hastighet	Snabb	Långsam

Tabell 2 Jämförelse mellan symmetrisk och asymmetrisk kryptering [1]

3. Säkerhet och säkerhetshot

Säkerhet handlar om skydd mot olika faror. Detta skydd kan utgöras av kryptering som skydd mot intrång, minskning av signalnivåer för att förhindra upptäckt av nätverket eller att nätverket bara används när det behövs och inte alltid är igång. En annan skyddsmetod är autentisering. Autentisering kan appliceras på både användare och meddelanden. Med användarautentisering avses kontroll av att en användare är den denne utger sig att vara och meddelandeautentisering innebär att man kontrollerar att meddelandet inte förändrats efter det skickats. [4]

Eftersom trådlösa nätverk i mångt och mycket fungerar som vanliga nätverk, bortsett från överföringsmetoden, så är även de attacker som kan utföras mot trådlösa nätverk i många fall samma som de som används mot vanliga sådana. Det finns dock vissa skillnader och dessa handlar framförallt om tillgängligheten till själva nätverket. Trådlösa nätverk är mer sårbara än vanliga nätverk då de använder sig av radiovågor istället för kablar för sin kommunikation. Säkerhet för vanliga nätverk har handlat mycket om att fysiskt skydda detta, exempelvis genom att det finns i en låst byggnad, vilket inte är möjligt för trådlösa dito. Vem som helst som är tillräckligt nära kan ansluta sig till nätverket. [4, 5]

3.1 Pfleegers säkerhetsmodell

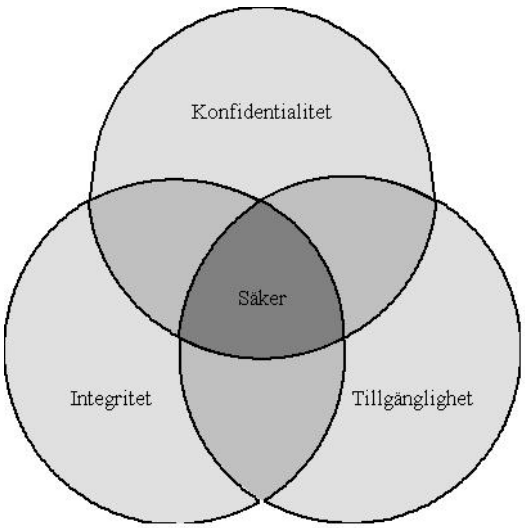
Pfleeger [1] talar om tre beståndsdelar som behövs för att datorsystem och nätverk ska anses vara säkra. Dessa är konfidentialitet, integritet och tillgänglighet.

- Konfidentialitet ska förhindra att obehöriga skaffar sig tillgång till datorrelaterade tillgångar eller information.

- Integritet innebär att endast de som är behöriga ska kunna ändra information och då enbart på ett godkänt vis. Att ändra informationen innefattar att skriva, skapa, radera och ändra status på denna.

- Tillgänglighet slutligen innebär att endast godkända personer kommer åt tidigare nämnda tillgångar och att de verkligen kommer åt dem. Man vill alltså skydda sig mot att en inkräktare hindrar användare från att få tillgång till systemet, så kallad denial of service (se 3.2).

Även om dessa tre är oberoende av varandra så behöver det, för att få ett säkert system, finnas en balans mellan dem. Det ena får inte utesluta det andra. Exempelvis så kan ett för starkt skydd av konfidentialiteten begränsa tillgängligheten. Se figur 3 för illustration.



Figur 3 Konfidentialitet, integritet, tillgänglighet [1]

Konfidentialitet, integritet och tillgänglighet har alla på något sätt att göra med vem som har tillgång till nätverket eller informationen i detta och ska förhindra otillåten användning av dessa. Cole m.fl. [3] nämner ytterligare två egenskaper nämligen ansvarsskyldighet och oförnekbarhet[2].

- Ansvarsskyldighet är en metod för att hålla användarna ansvariga för sina handlingar. Detta kan göras genom identifiering och autentisering av användarna samt att säkerhetsrelaterade händelser kan spåras.

- Oförnekbarhet innebär att en användare inte ska kunna förneka sina handlingar. Detta för att bevis ska finnas för att en händelse verkligen inträffat. Ett exempel på detta kan vara en digital signatur som verifierar för mottagaren att ett dokument skickats av en viss avsändare.

3.2 Attacker
Det finns många sätt att attackera trådlösa nätverk, allt från primitiva attacker till väldigt sofistikerade metoder. Jag kommer nedan att titta på några olika metoder som en inkräktare kan använda sig av för att skaffa sig tillgång till information eller nätverket som sådant. De flesta av dessa är inte unika för trådlösa nätverk utan fungerar även med trådade sådana. Man brukar skilja på fyra olika typer av attacker, men de flesta intrångsförsök består av en kombination av dessa: [4]

- Informationshämtning – Här hör man på namnet vad det handlar om. En inkräktare skaffar sig tillgång till information. Denna kan sedan användas antingen genom att informationen i sig utnyttjas eller i utpressningssyfte.

- Modifikation – Innebär att man ändrar innehåll i information som skickas. Kan utföras av flera skäl, till exempel vid banktransaktioner så att pengarna flyttas till andra konton än de avsedda eller att ändra IP-adress på datapaket så att de skickas till en annan mottagare.

- Maskering – Detta är attacker där man stjäl en annan användares identitet för att dölja sin egen. Detta kan vara till exempel MAC-adresser och IP-nummer. Fördelen med detta (för inkräktaren) är att säkerhetssystem inte upptäcker något konstigt utan ser det som vanlig trafik.

[2] Oförnekbarhet är ett svenskt uttryck för det engelska ordet nonrepudiation och används i detta sammanhang.

- Blockering – Denna metod skiljer sig från de övriga på så sätt att syftet med dem har varit att skaffa sig själv tillgång till information medan syftet med en blockering är att se till så att andra användare inte kommer åt en resurs av något slag. Denna metod kallas på engelska för Denial of Service och kommer att studeras mera utförligt nedan.

Denial of Service
Denial of Service (DoS) är en typ av attack som utförs för att påverka tillgängligheten hos ett nätverk eller en tjänst. Istället för att själv försöka ta sig in på nätverket så ser man till att ingen annan kan göra det. Ett vanligt sätt att utföra en sådan här attack är att överösa datorn som är målet för attacken med förfrågningar så att den inte kan svara på vanlig trafik eller att det går så långsamt att den ändå inte går att använda. Det finns flera olika typer av DoS-attacker. Målet är alltid att begränsa eller förhindra tillgänglighet men tillvägagångssätten skiljer sig åt. En typ av DoS-attack är en så kallas SYN flood. En vanlig TCP/IP-session mellan en klient och en server startar med en handskakning där klienten skickar ett SYN (synchronize)-meddelande till servern för att starta kommunikationen. Servern svarar då med både ett ACK (acknowledge) och ett SYN och klienten avslutar det hela med att skicka tillbaka ett ACK till servern. Efter detta är handskakningsprocessen avslutad. Efter att servern skickat SYN+ACK till klienten så sparar den ett sekvensnummer för den anslutningen tills den fått svar igen i form av ett ACK. Då handskakningen vanligtvis går fort är inte utrymmet där sekvensnumren sparas speciellt stort. Själva attacken går ut på att klienten skickar ett stort antal SYN till servern och sedan inte skickar något ACK på de svar som fås från servern. Då kommer utrymmet där servern sparar sekvensnumren att ta slut och den blir oförmögen att ta emot fler anslutningar. En variant på den precis nämnda metoden och som ofta används tillsammans med denna är att använda en falsk IP-adress i SYN-meddelandet. Detta görs av två anledningar; dels för att man inte vill avslöja sin egen IP-adress dels för att servern då inte kommer att få något svar.

En variant av DoS-attack är en Distribuerad DoS (DDoS) där flera datorer används samtidigt för attacken. Den fungerar i två steg där det första steget är att infektera de datorer som senare kommer att användas för attacken. Det kan till exempel göras med en *trojan*, som är ett program som verkar vara legitimt men som istället smittar datorn där det installeras. Detta upprepas sedan med ett stort antal datorer. De datorer som smittats kallas sedan för zombier. Det andra steget innebär att den som utför attacken vid en lämplig tidpunkt sätter igång denna genom att skicka en signal till alla zombier att de ska sätta igång attacken eller alternativt så är datum och tid bestämd redan från början. Den angripna datorn får då betydligt mer trafik att ta hand om. Det är också svårare att avbryta attacken samt att spåra källan för denna jämfört med en vanlig DoS-attack.

En variant på DDoS är en reflektorattack som innebär att den som utför attacken skickar en förfrågan till ett stort antal datorer som då kommer att besvara denna. Ett exempel på en sådan förfrågan skulle kunna vara ett SYN-meddelande som beskrivit ovan. Avsändarens IP-adress i förfrågan förfalskas så att den sätts till den adress som ska attackeras. När sedan svaren på alla förfrågningar som skickades kommer så kommer den attackerade datorn att överbelastas.
[1, 3, 30]

Social manipulation
Social manipulation är inte en attack på det sätt som övriga metoder som beskrivs här är. Här är det inte datorer eller nätverk som är målet för attacken utan människor. Social manipulation går ut på att använda social kompetens för att komma åt värdefull information eller att få anställda på företaget att utföra något som underlättar en attack. Detta görs exempelvis genom att ringa upp IT-avdelningen på ett företag som man vill skaffa sig information om och utge sig för att vara anställd, gärna högt uppsatt så att man inte blir ifrågasatt, och sedan hitta på en anledning för att ändra sitt lösenord. Det går också att vända på det hela så att inkräktaren ringer upp en anställd på företaget och säger att han ringer från IT-avdelningen och behöver ha tillgång till personens användarnamn och lösenord. Inkräktaren kan också be personen ifråga att utföra något kommando och sedan läsa upp resultatet. En ytterligare metod kan vara att gå igenom pappersavfall från företaget och där försöka hitta någon

relevant information. Det finns många möjligheter att skaffa sig information på och det bästa sättet att skydda sig mot sådana här incidenter är utbildning och klara regler för hur dessa frågor ska skötas. [1,3]

Man-in-the-middle
En man-in-the-middle-attack är en typ av attack där en inkräktare avlyssnar och möjligtvis förändrar kommunikationen mellan avsändare och mottagare. Både avsändare och mottagare tror att de kommunicerar direkt med varandra men istället så tar inkräktaren emot informationen från avsändaren, gör eventuellt någonting med den och skickar den sen vidare till mottagaren. Ett exempel på en sådan här attack skulle kunna vara då en part skickar över sin publika nyckel till en annan part för att de ska kunna kommunicera säkert. Om en inkräktare då snappar upp denna och istället skickar ett meddelande med sin egen publika nyckel (som ser ut att komma från den ursprungliga avsändaren) kan inkräktaren fortsättningsvis ta emot meddelandena från den part som tagit emot dennes nyckel. Dessa kan sedan dekrypteras, läsas och eventuellt modifieras innan de krypteras med avsändarens publika nyckel, som snappades upp tidigare, och sedan skickas vidare till denne. Varken avsändare eller mottagare märker att inkräktaren finns där. Fall där detta skulle kunna vara intressant (för inkräktaren) är banktransaktioner och Internet-handel. [1]

Avlyssning
En inkräktare kan ganska enkelt avlyssna trafiken i ett trådlöst nätverk genom att övervaka de radiovågor som skickas. Detta kan göras med hjälp av ett så kallat sniffer-program. Ett sådant program kan fånga upp de paket som skickas över nätverket och analysera dess innehåll. Genom att också använda en antenn kan man fånga upp kommunikationen på längre avstånd. [4, 32]

Förfalskning av MAC-adress
En accesspunkt kan spärras så att endast användare med godkända MAC-adresser tillåts ansluta sig. Genom att använda sig av program för avlyssning kan en inkräktare snappa upp trafik i nätverket och därigenom få tillgång till MAC-adressen för en dator som har tillgång till nätverket. Sedan kan andra program användas för att förfalska sin egen så att den motsvarar en godkänd adress. [33]

Evil twin
En ”evil twin”-attack är en attack där en inkräktare upprättar en bluff-accesspunkt i närheten av en riktig sådan. Bluff-accesspunkten kan bestå av en bärbar dator med ett trådlöst nätverkskort och programvara. Accesspunkten kan sedan ges ett namn som liknar den riktiga för att användarna inte ska misstänka något. Genom att inkräktarens accesspunkt är närmare offren än den riktiga kan signalen från denna bli starkare och därmed locka till sig fler användare. Datorn som används för bluff-accesspunkten kan ställas in så att kommunikationen bara går igenom denna, där den avlyssnas, och sedan vidare till den riktiga accesspunkten. Program för detta finns att ladda ner från Internet. Lämpliga miljöer att utföra en sådan här attack är där det finns fri trådlös uppkoppling som till exempel på flygplatser eller kaféer. [31]

4. Säkerhetslösningar

I detta kapitel kommer de tre säkerhetslösningarna WEP, WPA och WPA2 för trådlösa nätverk att gås igenom, hur de fungerar och vad som skiljer dem åt.

4.1 WEP

WEP som är en förkortning av Wired Equivalent Privacy är en krypteringslösning för att säkra trådlösa nätverk av standarden IEEE 802.11. Den kom 1999 och var tänkt att göra trådlösa nätverk lika säkra som vanliga trådade gällande konfidentialitet. 2001 framkom det att algoritmen hade flera svagheter och 2003 ersattes den av WPA, som kommer att beskrivas längre fram. I samband med att WPA2 ratificerades 2004 ansågs WEP förlegad och rekommenderas inte längre att användas. WEP används dock fortfarande och är ofta det första valet gällande säkerhet som visas när man installerar en ny router varför det finns intresse av att titta på algoritmen. WEP försöker leva upp till de tre säkerhetsfunktionerna konfidentialitet, autenticitet och integritet. Konfidentialitet i form av kryptering, autenticitet via kontroll av vilka klienter som får ansluta till nätverket och integritet genom integritetskontrollalgoritmen CRC-32. [4, 22]

Kryptering

WEP använder sig av krypteringsalgoritmen RC4 som är en symmetrisk algoritm för att autentisera klienter och kryptera data. Att algoritmen är symmetrisk innebär, som beskrivits tidigare, att både avsändare och mottagare använder samma nyckel. Avsändare och mottagare är i det här fallet klienten som använder det trådlösa nätverket och den accesspunkt som klienten använder sig av. WEP använder sig av en *initialiseringsvektor* som är ett block av bitar och används för att skapa en unik nyckelström som skiljer sig från andra nyckelströmmar skapade av samma nyckel. En nyckelström är en sekvens av slumpmässiga tecken. Meningen med initialiseringsvektorn är att försvåra kryptoanalys mot WEP genom att klienten använder olika initialiseringsvektorer och därmed olika nycklar för krypteringen av varje paket. Detta eftersom den symmetriska nyckeln sällan ändras. Initialiseringsvektorn sänds i klartext i paketet. Krypteringen i WEP fungerar på följande vis:

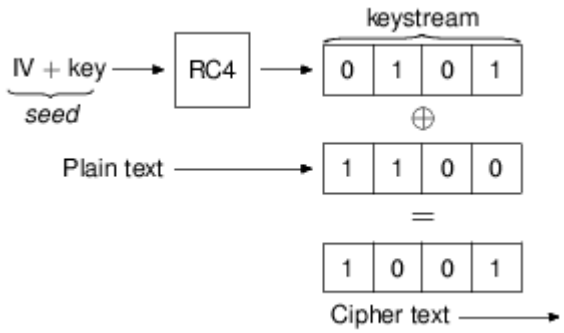
1. Initialiseringsvektorn som är 24 bitar lång kombineras med WEP-nyckeln som är 40 bitar lång för att tillsammans generera en 64-bitars nyckel som används av RC4-algoritmen. Algoritmen använder sedan RC4-nyckeln för att skapa en nyckelström vilken är lika lång som datan som ska krypteras.

2. Till datan som ska krypteras läggs ett ICV (Integrity Check Value). Detta är ett 4 byte långt kontrolltal. Talet används för att kontrollera att den krypterade datan inte förändrats under överföringen. Uträkningen av detta tal görs av CRC-32. Både datan som ska skickas och kontrolltalet ICV krypteras.

3. Nyckelströmmen och data + ICV, vilka är lika långa, kombineras sedan med en XOR-operation som ger krypterad strömmad data. Initialiseringsvektorn skickas med okrypterad.

4. När mottagaren, accesspunkten, tar emot ett paket sammanfogas den gemensamma nyckeln (som båda känner till) tillsammans med initialiseringsvektorn i det mottagna paketet och använder denna nyckel för att dekryptera paketet.

Det finns också WEP-kryptering med 128 bitar. Initialiseringsvektorn är fortfarande 24 bitar medan WEP-nyckeln nu är 104 bitar lång. I övrigt fungerar det på samma sätt som beskrivits ovan.
[4, 22, 23, 24]



Figur 4 WEP-kryptering [22]

Autentisering
WEP stöder två olika autentiseringsmetoder för att endast behöriga användare ska kunna ansluta till en accesspunkt; öppen och delad nyckel. Öppen autentisering fungerar som så att en klient begär autentisering och accesspunkten svarar att det lyckades. Detta innebär att det i praktiken inte sker någon autentisering. Den andra metoden, delad nyckel, använder WEP för autentisering genom en fyrvägshandskakning. Det fungerar enligt nedan:

1. Klienten sänder en förfrågan om autentisering till accesspunkten.

2. Accesspunkten skickar tillbaka en okrypterad utmaning.

3. Klienten krypterar utmaningen med WEP-nyckeln och skickar tillbaka den till accesspunkten.

4. Accesspunkten dekrypterar svaret från klienten och jämför det med den klartext som skickades först. Om dessa överensstämmer blir klienten godkänd, annars inte.

[4, 22]

Svagheter
Som nämnts tidigare så finns det stora säkerhetsproblem med WEP varför man inte bör lita på ett nätverk som är skyddat enbart med WEP. Jag ska här nämna några av de saker som gör WEP osäkert. [2, 4]

- Om man använder sig av öppen autentisering så räcker det att en klient anger ett SSID för att kunna koppla upp sig mot en accesspunkt. Då detta ibland sänds ut i klartext av accesspunkten så kan det enkelt kommas över av en inkräktare. Man kan begränsa åtkomsten till nätverket genom att endast ge klienter med godkända MAC-adresser tillgång till detta. Men då det är enkelt att förfalska en MAC-adress ger inte detta något egentligt skydd.

- Återanvändande av nyckelströmmarna är ett annat problem. Detta gäller alla system som använder sig av strömmade data. Problemet ligget i att XOR-operationen, som beskrivits ovan i samband med krypteringen, också fungerar baklänges. Detta innebär att om en inkräktare genom avlyssning fått tillgång till den krypterade informationen och också har tillgång till antingen datan eller nyckelströmmen så kan denne använda XOR-operationen för att komma fram till den del som saknas. Alltså, har han nyckelströmmen kan han komma fram till datan och vice versa. Detta ska initialiseringsvektorn hjälpa till att förhindra men det är inget krav (i standarden) att denna ska förändras. Initialiseringsvektorn skickas ju dessutom med paketet i klartext som beskrivits ovan. Om en inkräktare avlyssnar två olika paket innehållande samma initialiseringsvektor är det sannolikt att samma WEP-nyckel använts. Då slumpvalsfunktionen för initialiseringsvektorn ofta utformats på ett enkelt sätt så kan inkräktaren samla information där denna återanvänts. Genom kunskapen om initialiseringsvektorn och att nyckeln inte förändras tillsammans med kunskap om hur nyckeln kombineras med datan så har inkräktaren

tillräckligt med information för att med hjälp av automatiserade verktyg kunna knäcka algoritmen.

- Ett problem med initialiseringsvektorn är att den bara är 24 bitar. Detta innebär att 2^{24} eller cirka 17 miljoner unika nyckelströmmar kan fås fram. I ett vältrafikerat nätverk innebär det att nyckeln kommer att upprepas med några timmars mellanrum. En inkräktare som avlyssnar trafiken och hittar två paket med samma initialiseringsvektor kan då försöka komma åt innehållet på det sätt som beskrivs i punkten ovan.

- Integritetskontrollen fungerar inte då en inkräktare som har tillgång till WEP-nyckeln kan ändra innehållet i ett paket och sedan återskapa integritetskontrollen. Det är alltså möjligt att ändra ett meddelande utan att mottagaren upptäcker detta.

4.2 WPA

WPA (Wi-Fi Protected Access) är en standard som tagits fram av Wi-Fi Alliance och kom som en följd av de säkerhetsproblem som upptäcktes hos WEP. 2003 tillkännagav Wi-Fi Alliance att WPA tagit över efter WEP. WPA är en delmängd av 802.11i-standarden. Den kom som en dellösning innan hela 802.11i-standarden var färdig. Det finns två olika varianter av WPA: enterprise och personal. Skillnaden mellan dessa är att enterprise använder sig av en autentiseringsserver och 802.1x där varje användare får olika nycklar medan personal har ett gemensamt lösenord som används av alla datorer som ansluter. Krypteringen av data görs med hjälp av RC4 som är samma algoritm som användes i WEP. En 128 bitars nyckel används tillsammans med en 48 bitars initialiseringsvektor att jämföras med initialiseringsvektorn i WEP som bara var 24 bitar. Dessutom har en kontroll införts för vilka värden som används som initialiseringsvektor. Det är detta som gör att RC4 kan användas i WPA också. En klar förbättring jämfört med WEP är TKIP, ett säkerhetsprotokoll som dynamiskt ändrar nycklar under tiden som systemet används. TKIP beskrivs utförligare nedan. Det ska dock nämnas att det går att knäcka WPA-kryptering idag. [4, 25]

TKIP

TKIP (Temporal Key Integrity Protocol) är ett säkerhetsprotokoll som används i IEEE 802.11-nätverk. Det togs fram av Wi-Fi Alliance som en lösning för att slippa byta ut gammal hårdvara vid en övergång från WEP till WPA. TKIP kan liknas vid ett skal som ligger runt den äldre WEP-standarden. Detta för att uppnå bättre säkerhet gällande kryptering. TKIP är uppgraderad på följande sätt jämfört med WEP:

Paketnycklar

Denna funktion tar hand om problemet som WEP har med svaga nycklar genom att ändra nyckeln för varje paket som sänds. En temporär nyckel skapas utifrån den huvudnyckel som översändes vid autentiseringen. Genom att använda en XOR-operation på datorns eller accesspunktens MAC-adress och den temporära nyckeln skapas en ”mellan-nyckel”. Eftersom den bygger på MAC-adressen så kommer olika datorer och accesspunkter att generera olika mellan-nycklar. Denna mellan-nyckel används sedan tillsammans med sekvensnumret för paketet för att ta fram en paketnyckel och initialiseringsvektor. Detta döljer förhållandet mellan nyckeln och initialiseringsvektorn. Paketnyckeln är 128 bitar lång och består av en 104 bitars RC4-nyckel och en 24 bitars initialiseringsvektor (24 av initialiseringsvektorns 48 bitar väljs ut). Denna används sedan som grund för WEP-krypteringen. Det är hur nyckeln skapas och hanteras som är det nya och åtgärdar det problem som WEP hade med återanvändning av initialiseringsvektorn. Att man använder en ny nyckel för varje paket gör det svårt för en inkräktare att dekryptera informationen.

Sekvenskontroll

Den tidigare nämnda förlängda initialiseringsvektorn som är 48 bitar lång baseras på en räknare som kallas TSC (TKIP Sequence Counter). Eftersom TSC uppdateras med varje paket kan 2^{48} paket skickas med unik temporär nyckel innan denna upprepas. Detta tar väldigt lång tid och innebär därför inte något problem. Som skydd mot återsända eller förfalskade paket (replay-attacker) använder TKIP en sekvenskontroll där mottagaren kan kontrollera om ett paket som mottagits kommit i fel ordning. Om så är fallet är risken att en inkräktare skickat om ett redan sänt meddelande. Mottagaren kastar då paketet. Ett paket anses vara inkommet i fel ordning om dess initialiseringsvektor är mindre än eller lika med en initialiseringsvektor för ett paket som tidigare tagits emot. Genom att använda WEP-nyckelns initialiseringsvektor som sekvensnummer kan en replay-attack upptäckas på följande vis:

1. Nya TKIP-nycklar används

2. Avsändare och mottagare initierar paketsekvensnumret till noll

3. För varje paket som skickas ökas sekvensnumret av avsändaren

4. Den ovan beskrivna proceduren används för att avgöra om ett paket kommit i fel ordning (vilket skulle innebära att ett återsändande inträffat)

Message Integrity Codes
Ett problem som finns med WEP är hur ICV (integritetskontrollvärde) för varje paket räknas ut. Detta används för att kontrollera att datan som skickas inte förändras under överföringen. Det går dock att komma förbi detta. Ett säkrare sätt att kontrollera detta är med en MIC (Message Integrity Code) som är en unik representation av meddelandet som skickas, en slags checksumma. Denna kommer att förändras om bitarna i meddelandet förändras. Avsändaren av meddelandet räknar ut en MIC med hjälp av en nyckel som endast avsändaren och mottagaren känner till. Denna skickas sedan tillsammans med meddelandet. Mottagaren kan sedan räkna ut en ny MIC baserad på meddelandet och jämföra denna med den som skickades med meddelandet. Stämmer dessa två överens så har meddelandet inte förändrats under vägen. I TKIP kallas MICen som är 64 bitar för Michael.
[3, 4, 26]

Autentisering med 802.1x och EAP
802.1x är en IEEE-standard som tagits fram för att öka säkerheten för trådlösa nätverk. Den använder sig av TKIP för integritet och EAP för autentisering av användare. EAP (Extensible Authentication Protocol) är ett ramverk för autentisering som kan användas för trådlösa nätverk. Anledningen till att EAP används är att 802.1x inte innehåller någon autentiseringsmetod. Det används i det här sammanhanget för att erbjuda en säker autentiserings-mekanism vilket beskrivs nedan.

Kommunikationen börjar med att klienten försöker ansluta till accesspunkten. Accesspunkten öppnar då en port för kommunikation med EAP-paket mellan klienten och en autentiseringsserver. Ingen annan trafik mellan klienten och accesspunkten är tillåten förrän klienten blivit godkänd av autentiseringsservern. Autentiseringen fungerar på följande sätt:

1. Klienten som vill ansluta skickar ett startpaket (EAP) till accesspunkten.

2. Accesspunkten svarar med en EAP-förfrågan för att få mer information om klienten.

3. Klienten svarar med ett EAP-paket innehållande information om sig själv. Denna vidarebefordras av accesspunkten till autentiseringsservern.

4. Autentiseringsservern kontrollerar att klienten är den som den utger sig att vara, till exempel via ett certifikat. Blir klienten godkänd skickas ett godkännande till accesspunkten.

5. Accesspunkten skickar ett EAP-paket till klienten att denne är godkänd.

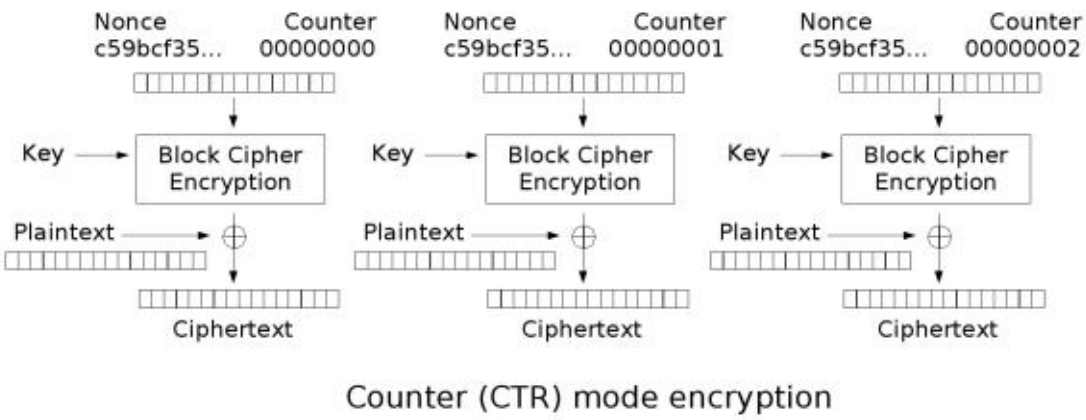
En huvudnyckel skickas sedan till både klienten och accesspunkten. En fyrvägshandskakning där klienten och accesspunkten bekräftar varandra och installerar nycklar avslutar processen. [3, 26, 27]

PSK (Pre Shared Key)
WPA-PSK är en annan variant av WPA som skiljer sig från WPA-TKIP på så sätt att man inte använder sig av en autentiseringsserver. Detta är vanligt för privatpersoner eller mindre företag som inte har tillgång till en sådan. Istället anges ett lösenord manuellt för varje klient som vill ansluta sig till nätverket. Säkerheten beror då på hur pass bra detta är. Lösenordet kan sparas hos klienten för att slippa ange det manuellt varje gång. Lösenordet måste minst vara 8 tecken långt men bör vara minst 20 för att anses vara säkert. [25]

4.3 WPA2
WPA2 som är den fullständiga implementationen av standarden 802.11i kom under 2004. WPA2 finns liksom WPA i två varianter; enterprise och personal och skillnaderna dem emellan är de samma som för WPA-varianterna. En skillnad jämfört med WPA är att en ny krypteringsalgoritm, CCMP, tillkommit. Från och med mars 2006 krävs WPA2 för alla nya enheter som vill bli Wi-Fi-certifierade. Det krävs en del för att uppgradera från WPA till WPA2 och därför är det inte många som tagit steget. Använder man sig av nyare utrustning är det möjligt att det går att uppdatera hårdvaran med hjälp av firmware (mjukvaruuppdatering) medan det för äldre produkter saknas denna möjlighet då de inte har kapacitet att hantera de nya, mer krävande, krypteringsalgoritmerna (som kräver mer beräkningskapacitet). Detta var inget problem när det gällde uppdateringen från WEP till WPA då de använde sig av samma algoritm. [4, 25]

Kryptering
I WPA2 tillkommer en ny krypteringsmetod utöver TKIP som används i WPA som kallas AES-CCMP. AES är en förkortning av Advanced Encryption Standard och är ett blockkrypto som använder sig av 128 bitar stora block. Informationen som ska krypteras delas alltså upp i 128 bit stora block innan kryptering. CCMP (Counter mode CBC-MAC Protocol) är en sammanslagning av tre förkortningar: CTR, CBC och MAC. CTR står för Counter Mode Encryption, CBC för Cipher Block Chaining och MAC för Message Authentication Code. CTR är en metod för informationskryptering medan CBC-MAC är en metod för hur integritetskontrollen skapas. För CCMP används en 128-bitars nyckel.

Krypteringen fungerar på följande vis: skulle inte klartexten vara jämt delbar med 128, vilket krävs på grund av blockstorleken på 128 bit, så ordnar CCMP detta genom att genom att lägga till godtycklig data. Denna tas sedan bort igen vid dekryptering. En räknare, som räknas upp för varje block, adderas med ett nonce (number used once) som är ett slumptal. Både startvärdet på räknaren och värdet som den ökas med ändras för varje paket som krypteras. Detta för att försvåra för en eventuell inkräktare. Noncen skapas av CCMPs motsvarighet till initialiseringsvektor, PN (Packet Number) som är 48 bitar lång. CTR lägger sedan noncen och räknaren till AES temporära nyckel och en XOR-operation utförs på klartexten för att skapa kryptotexten.



Figur 5 CTR-kryptering [41]

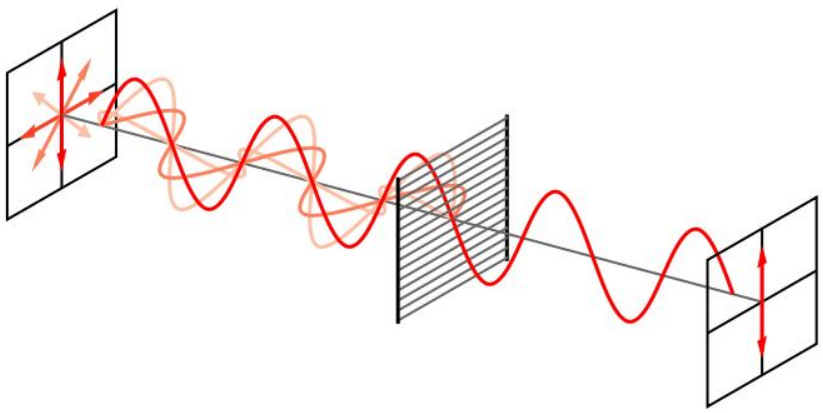
Integritet och autentisering
För att upprätthålla integriteten krävs ett sätt för två enheter att kunna kontrollera att ett meddelande inte förändrats efter att det skickats. Detta sköts av CBC-MAC och fungerar som så att det första 128-bitblocket med data krypteras med AES. Kryptotexten används sedan med en XOR-operation på det andra 128-bitblocket. Detta fortsätter tills ett MIC-värde räknats ut för hela meddelandet och man har då fått en MIC i form av ett 128 bitars block. Det är dock bara de första 64 bitarna som används till MICen, resten kastas bort. Chansen att en inkräktare skulle lyckas förfalska MICen är 1 på 10^{19} och därmed anses integriteten säkrad. Beräkningen av MIC och krypteringen av meddelandet utförs parallellt. Autentisering fungerar på samma sätt som beskrivits för WPA med hjälp av 802.1x och EAP eller PSK. [4, 28, 29]

5. Kvantkryptering

Kvantkryptering har funnits sen 80-talet då en fysiker vid namn Stephen Wiesner och två datavetare, Charles Bennett och Gilles Brassard, utförde försök med att använda sig av kvantmekaniska principer i samband med kryptering. Kvantkryptering är en krypteringsteknik som bygger på kvantmekaniska metoder. Kvantmekaniken behandlar naturlagar i system av mikroskopisk storlek såsom molekyler, atomer och atomkärnor. Kvantkrypteringen skiljer sig därmed från andra krypteringstekniker som bygger på matematik. Kvantkryptering anses vara den enda krypteringsmetod som inte går att knäcka. Kryptering med en engångsnyckel förutsätter att båda sändare och mottagare har tillgång till varsin kopia av samma sträng med oförutsägbara nummer. Problemet med denna metod är vad man ska använda som källa för krypteringen. Ett annat problem är hur man på ett säkert sätt ska överföra nyckeln så att ingen som tjuvlyssnar på kommunikationen ska komma åt den. Kvantkryptering tar hand om båda dessa problem vilket vi kommer att se längre fram. Kvantkryptering eller kvantnyckelöverföring (quantum key distribution) som det också kallas används enbart till att ta fram och överföra en nyckel. Det används alltså inte för den fortsatta krypteringen utan då använder man istället den översända nyckeln på vanligt vis. [1, 34, 35, 36]

5.1 Fotoner och polarisation

En foton är en ljuspartikel och namnet kommer från grekiskans ord för ljus, phos. De rör sig genom luften (eller vakuum) med en bestämd riktning och bär med sig en bestämd mängd energi. Ljus har enligt kvantteorin både våg- och partikelegenskaper. Fotoner vibrerar i alla riktningar när de förflyttar sig. Polarisation är en fysisk egenskap hos elektromagnetiska vågor, till exempel ljus, som har att göra med hur fotonen rör sig genom luften. Även om fotoner kan ha vilken riktning som från 0° till 360° så utgår man inom kvantkrypteringen från fyra olika riktningar nämligen 0° (↑), 45°(↗), 90°(→) och 135°(↘). Riktningen på en fotons polarisation kan styras till en bestämd sådan med hjälp av ett polarisationsfilter (se figur 6 nedan). [1, 34]



Figur 6 Användning av polarisationsfilter [37]

5.2 Nyckeldistribution med BB84

BB84, uppkallat efter sina uppfinnare Bennett och Brassard samt det år det publicerades, är ett protokoll som låter två deltagare utbyta en nyckel med hjälp av polariserade fotoner. Avsändare och mottagare kommunicerar via två kanaler, en ”kvantkanal” som kan vara en optisk fiber för att överföra fotonerna och en traditionell som Internet. Ingen av kanalerna behöver vara säker då protokollet i sig utgår från att det kan vara avlyssnat och att en inkräktare kan störa kommunikationen i båda kanalerna. Två baser bestäms där en bas är ett par av ortogonala (vinkelräta) tillstånd. Baserna som används här är 0° och 90° samt 45° och 135° (se nedan). Det fungerar på följande vis:

Bas	0	1
+	↑	→
X	↗	↘

Tabell 3 Baser [36]

1. Avsändaren tar fram en binär slumpsekvens av bitar.

2. Avsändaren bestämmer vidare vilken bas som ska användas för varje bit i sekvensen.

3. Avsändaren skickar en sekvens av polariserade fotoner vars polarisation representerar bitarna i sekvensen.

4. Avsändaren skickar sekvensen av fotoner till mottagaren över en kvantkanal.

5. För varje foton som mottagaren tar emot gissar denne vilken bas som använts, rätlinjig eller diagonal, och ställer in sin utrustning därefter.

6. Mottagaren mäter varje foton utifrån den bas som valdes i föregående steg vilket genererar en ny bitsekvens.

7. Avsändaren och mottagaren kommunicerar sedan över en vanlig kanal. Avsändaren berättar då för mottagaren vilken bas som användes för varje bit och mottagaren kontrollerar vilket val han gjorde på motsvarande bit. De bitar där de inte gjorde samma val används inte.

Avsändarens slumpade bit	0	1	1	0	0
Avsändarens bas	+	+	X	+	X
Avsändarens polarisation	↑	→	↘	↑	↗
Mottagarens bas	+	X	X	X	X
Mottagarens polarisation	↑	↗	↘	↗	↗
Bitar som används till nyckel	0		1		0

Tabell 4 Exempel på nyckeldistribution [36]

Det är alltså endast om mottagaren gissat rätt gällande vilken bas som använts som mätningen blir korrekt. Skulle till exempel en linjär mätning utföras på en diagonalt polariserad foton så kommer resultatet att bli slumpmässigt 0 eller 1. Då det är 50 % chans att mottagaren väljer rätt filter (linjärt eller diagonalt) så är sannolikheten att denne kommer att gissa rätt på samtliga fotoner $0{,}5^n$ där n är antalet fotoner som skickats. Kommunikationen under punkt 7 kan ske helt öppet eftersom man inte avslöjar något om biten som sänts utan enbart om vilka baser som använts. [34, 36]

5.3 Att upptäcka inkräktare

Säkerheten inom kvantkryptering bygger på att man inte kan avlyssna kommunikationen utan att påverka den. BB84-protokollet använder sig av *Heisenbergs osäkerhetsprincip* för att upptäcka avlyssning. Denna princip säger att det inte är möjligt att mäta både positionen och hastigheten hos en partikel samtidigt eftersom om vi mäter hastigheten så har positionen förändrats och vice versa. Ett par som det inte går att mäta värdet på samtidigt kallas konjugatvariabler. Inom kvantkrypteringen är det den rätlinjiga och diagonala polarisationen som används som konjugatvariabler. Om man, som nämnts ovan, försöker mäta en diagonalt polariserad foton med ett rätlinjigt filter förlorar man informationen som fotonen innehåller. Då en inkräktare som avlyssnar kommunikationen inte vet vilken typ av foton som används för varje bit måste denne gissa vilken bas som ska användas. Eftersom en avlyssning kommer att påverka fotonen så måste inkräktaren skapa en ny foton att skicka

vidare till mottagaren. Detta kommer att störa fotonströmmen så pass mycket att avsändare och mottagare enkelt upptäcker det. Det kan gå till på följande sätt: [1, 34]

1. Avsändaren vill sända sekvensen 00110 till mottagaren.
2. Han väljer baser vilket ger fotoner med polarisation enligt tabellen nedan.
3. Inkräktaren väljer också baser enligt tabellen.
4. Inkräktaren snappar upp varje foton och mäter den efter sina basval enligt tabellen
5. Inkräktaren byter ut fotonerna genom att koda dessa med de baser som valdes i steg 3. En så kallad intercept-resend-attack.
6. Mottagaren tar emot fotonerna och mäter dem utifrån baser som denne väljer slumpmässigt.
7. Avsändare och mottagare jämför nu sina basval och upptäcker då, på den andra biten, att de blivit avlyssnade eftersom de hade samma baser men fick olika bit-värden.

Avsändare	Bit-sekvens	0	0	1	1	0
	Baser	+	X	+	X	X
	Skickade fotoner	→	↗	↑	↘	↗
Inkräktare	Baser	+	+	X	X	X
	Mätresultat	0	1	0	1	0
	Nya, skickade fotoner	→	↑	↗	↘	↗
Mottagare	Baser	+	X	X	+	X
	Mätresultat	0	1	0	0	0

Tabell 5 Upptäckt av inkräktare [34]

5.4 Privacy amplification och secret key reconciliation

Det krävs ett sista steg för att BB84-protokollet ska bli komplett. Problemet är att det finns skillnader mellan mottagarens och avsändarens nyckelsekvens. Dessa skillnader kan bero på en inkräktare som avlyssnat kommunikationen men det kan också bero på brister i utrustningen som används. Då det inte går att skilja på vad som orsakat felet utgår man, för säkerhets skull, från att alla felaktigheter beror på avlyssning. I två steg tar man först bort felaktiga bitar och sedan minskar man en eventuell inkräktares kännedom om nyckeln till ett godtyckligt litet värde. Sammanjämkningen av nyckeln (secret key reconciliation) är en procedur där avsändare och mottagare utför rättning av fel för att bådas nycklar ska bli identiska. Detta steg utförs öppet varför det är viktigt att så lite information som möjligt om nyckeln avslöjas för en eventuell inkräktare. Avsändaren och mottagaren delar upp sina bitsekvenser i block och jämför därefter varje block för sig. Så fort de hittar ett block som inte överensstämmer delas detta block upp i mindre block och man börjar om igen. När man hittat den felaktiga positionen så kommer avsändare och mottagare överens om de ska kasta biten eller om de ska bestämma ett korrekt värde. Då viktig information om nyckeln kan ha snappats upp av en inkräktare under nyckel-sammanjämkningen utförs ett steg som kallas ”privacy amplification”. Efter det föregående steget så har avsändare och mottagare en gemensam bitsekvens. Problemet är att några av dess bitar även kan vara kända av en inkräktare som kommit över dem antingen under nyckelöverföringen eller under nyckel-sammanjämkningen. För att bli av med detta måste de gemensamt förändra sina sekvenser till exempel genom en slumpmässig permutation det vill säga att de ändrar ordningen på bitarna. Därefter kastas en delmängd av dessa och används inte i den

slutgiltiga nyckeln. Hur mycket kortare nyckeln blir avgör även hur säker den är. Efter att dessa två steg utförts så har avsändare och mottagare en gemensam och hemlig bitsekvens. [34, 36]

5.5 Kvantkryptering i praktiken

Det som behövs för att det ska vara möjligt att använda kvantkryptering i praktiken är en fotonsändare, polarisationsfilter, en kvantkanal att sända över och en detektor. Kvantkanalen kan som beskrivits ovan bestå av en optisk fiber eller att man sänder genom luften. Då man sänder genom luften krävs det att man har fri sikt. För att skapa fotoner använder man sig av svaga laserpulser med ett lågt antal fotoner. För att kunna ta emot fotonerna använder man sig av lavindioder av till exempel kisel eller germanium vilka släpper ifrån sig elektricitet när de kommer i kontakt med fotoner. Problemet med de lasrar som används är att de är så svaga att i vissa pulser sänds det inga fotoner medan andra kan innehålla en eller två fotoner. Detta spelar ingen roll för funktionen då endast de fotoner som når mottagaren används. [38, 40]

Det finns idag åtminstone tre företag som tillverkar utrustning för kvantkryptering; id Quantique i Schweiz, MagiQ Technologies i USA och SmartQuantum i Frankrike. Flera andra företag har forskningsprojekt inom området. I åtminstone id Quantiques system är de ovan nämnda delarna samlade i en låda som ser ut som en vanlig datorlåda och används tillsammans med vanliga datorer och mjukvara. [36, 39]

Kvantkryptering har använts i skarpa fall. 2004 användes det för att föra över en check från borgmästaren i Wien till en österrikisk bank och i oktober 2007 användes det för att överföra valresultat från den schweiziska kantonen Genève till parlamentsbyggnaden.
De längsta avstånd som uppmätts för nyckelöverföringar är 148,7 kilometer genom optisk fiber och 144 kilometer genom etern (mars 2007). [36]

5.6 Attacker

Kvantkryptering med BB84 anses vara säkert såtillvida att en inkräktare som försöker avlyssna kommunikationen kommer att upptäckas. Ett exempel på detta tas upp ovan under 5.3. Det finns dock andra omständigheter som kan äventyra säkerheten. Dessa inkluderar att en inkräktare skaffar sig fysisk tillgång till apparaturen hos avsändare eller mottagare och utger sig för att vara någon av dessa. Detta kan avstyras genom autentisering som endast tillåter den rättmätige ägaren att använda utrustningen. Denial of Service är en annan metod som kan användas. Detta skulle kunna göras genom att kapa den optiska fibern eller, om man sänder genom luften, se till att blockera vägen. Ett annat effektivt sätt att utföra detta är genom att avlyssna kommunikationen då man tvingar de kommunicerande parterna att börja om. [34, 36]

Sammanfattning

Avsikten med detta arbete var att jag ville skaffa mig insikt i hur nätverk och säkerheten i dessa fungerar. Anledningen till att jag valde just trådlösa nätverk är att de redan används i stor utsträckning och jag tror att de kommer att användas ännu mer i framtiden. Folk blir mer och mer rörliga och vill kunna koppla upp sig överallt och alltid. Jag tror inte att vanliga trådade nätverk kommer att försvinna men användandet av dem kommer säkerligen att minska åtminstone bland privatpersoner. Bland företag tror jag de kommer att hålla fast vid vanliga nätverk under en längre tid.

Inledningsvis i uppsatsen togs grunderna upp angående vad ett trådlöst nätverk är och hur de fungerar. Organisationen IEEE och de olika varianterna av deras 802.11-standard för trådlösa nätverk gicks igenom. Vidare studerades TCP/IP-modellen som är en modell för datakommunikation över nätverk som till exempel Internet. I följande kapitel gjordes en genomgång av grunderna inom kryptering. Begrepp såsom nycklar och algoritmer gicks igenom, de två typerna av kryptering, symmetrisk och asymmetrisk gicks igenom och jämfördes. Block- och strömkrypton som är olika typer av symmetrisk kryptering beskrevs. De skiljer sig åt på så sätt att strömkrypton krypterar ett tecken i taget medan blockkrypton krypterar ett block, det vill säga flera tecken åt gången. Pfleegers säkerhetsmodell och de olika beståndsdelar i form av konfidentialitet, integritet och tillgänglighet som krävs för att ett nätverk ska anses vara säkert studerades. Olika typer av attacker gicks igenom och slutligen beskrevs några faktiska attacker .

För att skydda nätverket mot intrång krävs det att någon form av säkerhetslösning används. Även om man inte tycker att man har någon information som behöver hållas hemlig är det viktigt att se till att nätverket är skyddat så att det inte kan användas av obehöriga för att eventuellt utföra olagliga handlingar. I uppsatsen har tre olika säkerhetslösningar tagits upp: WEP, WPA och WPA2. WEP som är den som varit med längst anses idag undermålig och går att knäcka på bara ett par sekunder. WPA är den som, enligt min uppfattning, främst används idag åtminstone bland hemanvändare medan WPA2 kommer att ta över successivt. Utvecklingen går framåt hela tiden både vad gäller tekniker för att attackera trådlösa nätverk och de säkerhetslösningar som finns att tillgå. I takt med att datorer blir snabbare och nya säkerhetsluckor upptäcks kommer de säkerhetslösningar som anses säkra idag säkerligen inte att anses vara det om ett par år. Nya standarder och protokoll kommer att behöva tas fram för att möta de hot som komma skall.

Avslutningsvis togs kvantkryptering upp. Kvantkryptering är en metod för att med hjälp av fysiska lagar utbyta en nyckel för kryptering. Metoden har funnits sedan 80-talet men det är inte förrän på senare år som den använts praktiskt och den är fortfarande under utveckling.
Det kommer nog att dröja ett tag innan kvantkryptering används i någon större utsträckning. För det första känns inte tekniken mogen. De stora begränsningarna ligger i att avstånden som kvantkryptering kan användas över är för korta. För det andra är tekniken känslig för störningar oavsett om man sänder genom en fiberoptisk kabel eller genom luften. De jag i ett första skede kan se skulle kunna vara intresserade av att använda denna teknik är banker och andra (större) företag som hanterar känslig information. Jag har svårt att se att privatpersoner kommer att använda sig av kvantkryptering de närmaste åren.

7. Referenser

7.1 Böcker

[1] Pfleeger, Pfleeger. Security in Computing 3:e upplagan. Prentice Hall, 2003

[2] Stallings. Network Security Essentials 2:a upplagan. Prentice Hall, 2003

[3] Cole, Krutz, Conley, Reisman, Ruebush, Gollman, Reese. Network Security Fundamentals, Wiley Pathways 2008

[4] Olsson. Säkerhet i Trådlösa Nätverk. 4G Media, 2006

[5] Imai, Rahman, Kobara. Wireless Communications Security. Artech House, 2006

[6] Lindberg. Trådlösa nätverk – WLAN, WEP och Wi-Fi. Studentlitteratur, 2002

[7] Coulouris, Dollimore, Kindberg. Distrbuted Systems: Concepts and Design. Addison Wesley, 2005

7.2 Webbsidor

[8] http://en.wikipedia.org/wiki/Wireless_LAN, mars 2008

[9] http://en.wikipedia.org/wiki/Wi-Fi, april 2008

[10] http://wireless.industrial-networking.com/articles/articledisplay.asp?id=225, april 2008

[11] http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers, mars 2008

[12] http://en.wikipedia.org/wiki/IEEE_802.11, mars 2008

[13] http://en.wikipedia.org/wiki/IEEE_802.11i, mars 2008

[14] http://en.wikipedia.org/wiki/TCP/IP_model, april 2008

[15] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm, april 2008

[16] http://learn-networking.com/tcp-ip, april 2008

[17] http://www.di-mgt.com.au/cryptokeys.html, mars 2008

[18] http://en.wikipedia.org/wiki/Key_generation, mars 2008

[19] http://en.wikipedia.org/wiki/Key_%28cryptography%29, mars 2008

[20] http://sv.wikipedia.org/wiki/Asymmetrisk_kryptering, mars 2008

[21] http://en.wikipedia.org/wiki/Public-key_cryptography, mars 2008

[22] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy, mars 2008

[23] http://en.wikipedia.org/wiki/Initialization_vector, mars 2008

[24] http://en.wikipedia.org/wiki/Keystream, april 2008

[25] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, april 2008

[26] http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, april 2008

[27] http://www.wi-fi.org/files/wp_8_WPA%20Security_4-29-03.pdf, april 2008

[28] http://en.wikipedia.org/wiki/Cryptographic_nonce, april 2008

[29] http://www.sans.org/reading_room/whitepapers/wireless/1467.php, april 2008

[30] http://en.wikipedia.org/wiki/Denial-of-Service_attack, april 2008

[31] http://en.wikipedia.org/wiki/Evil_twin_%28wireless_networks%29, april 2008

[32] http://en.wikipedia.org/wiki/Packet_sniffer, april 2008

[33] http://en.wikipedia.org/wiki/Wireless_security, april 2008

[34] http://www.acm.org/crossroads/xrds11-3/qcrypto.html, april 2008

[35] http://www.ne.se/jsp/search/article.jsp?i_art_id=234268&i_word=kvantmekanik, april 2008

[36] http://en.wikipedia.org/wiki/Quantum_cryptography, april 2008

[37] http://en.wikipedia.org/wiki/Polarizer, maj 2008

[38] http://sfs.poly.edu/presentations/MikeSpres.pdf, maj 2008

[39] http://www.idquantique.com/products/files/clavis-specs.pdf, maj 2008

[40] http://www.idquantique.com/products/files/paper-industrial2005.pdf, maj 2008

[41] http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, maj 2008

[42] http://en.wikipedia.org/wiki/Stream_cipher, juni 2008

[43] http://en.wikipedia.org/wiki/AES_%28cipher%29, juni 2008

[44] http://en.wikipedia.org/wiki/Blowfish_%28cipher%29, juni 2008